jamk.fi

ICT-infrastruktuurin suunnitteluohje koulurakennuksiin

Aaro Liehu

Opinnäytetyö
Syyskuu 2019
Tekniikan ala
Insinööri(AMK), Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä	Julkaisun laji	Päivämäärä
Liehu, Aaro	Opinnäytetyö, AMK	2/2020
	Sivumäärä 98	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
ICT-infrastruktuurin suunnitteluohje koulurakennuksiin

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaajat
Sampo Kotikoski, Pasi Hakkarainen

Toimeksiantaja
Caverion Suomi Oy

Tiivistelmä

Pyrittiin parantamaan erilaisten talotekniikkajärjestelmien toimintaa tietoverkossa, sekä yhdistämään järjestelmäkokonaisuuksia yhteen suunnitteluohjeeseen. Pyrittiin parantamaan tietoverkkosuunnittelijoiden tietämystä erilaisista järjestelmistä, ja samaan aikaan parantamaan eri järjestelmien asiantuntijoiden tietämystä tietoverkoista. Tavoitteena oli luoda sellainen tietoverkon suunnitteluohje, jossa keskitytään erityisesti näiden järjestelmien toimintavarmuuteen ja suunnitteluun. Tarkoituksena oli myös yhdistää eri osa-alueiden asiantuntijoiden tietämystä yhteen suunnitteluohjeeseen. Tutkimuksessa suunniteltua esimerkki tietoverkkoa ei toteutettu eikä sen toimintaa testattu, mutta ohjeen tarkoituksena on antaa suuntaa suunnittelulle ja tutkimuksen ohje voisi olla jälkikäteen parannelta-vissa ja täysin muokattavissa.

Laadullinen tutkimus toteutettiin perehtymällä tarkemmin järjestelmiin sekä aiempiin toteutusratkaisuihin. Syvempää ymmärrystä järjestelmistä ja niiden vaatimuksista saatiin haastattelemalla eri osa-alueiden asiantuntijoita ja hyödyntämällä heidän käytännön kokemustaan.

Tutkimuksen tuloksena saatiin luotua alustava suunnitteluohje tietoverkolle keskittyen etenkin talotekniikkajärjestelmiin. Ohjeen toteutusmalleja ei kuitenkaan testattu käytännössä, joten se voi sisältää virheitä. Kuitenkin työn tarkoituksena oli tuottaa alustava malli tietoverkon suunnitteluohjeelle, jota voi kehittää ja parantaa jälkikäteen. Tähän tavoitteeseen päästiin.

Täydellisen tietoverkon ja sen toiminnan suunnittelu etukäteen voi olla hankalaa, ja toiminnan hiominen testausvaiheen jälkeen on tärkeää.

Avainsanat (asiasanat)

Infrastruktuuri, tietoverkko, suunnittelu

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author	Type of publication	Date
Liehu, Aaro	Bachelor's thesis	2/2020
		Language of publication: Finnish
	Number of pages 98	Permission for web publication: x

Title of publication

Instruction of ICT infrastructure design for school buildings

Degree programme

Information and Communication Technology

Supervisors

Sampo Kotikoski, Pasi Hakkarainen

Assigned by

Caverion Suomi Oy

Abstract

The goal was to improve the operation of building service systems in a local network and combine different systems in to one-design instruction. The goal was also to improve network designers' knowledge of different building service systems, and at the same time, help system specialists to understand networking better. The priority was to create a network design instruction targeting especially the operation and designing of building service systems. The purpose of the instruction was to unite many different subsectors in to one instruction. The planned example network was not deployed or tested; however, the idea of the instruction is to only give some direction about systems to specialists designing networks. The instruction is a base that can be developed and modified later.

Qualitative research was implemented by studying different systems and researching earlier deployments. A deeper understanding of the building service systems and their requirements was gained by interviewing different system specialists and utilizing their practical experience.

As a result of research, a tentative base of the network designing instruction was created which focuses on the building service systems. The network example configurations and deployments were not tested; hence, it is possible they could contain errors. However, the focus was on the creation of a base to a network designing instruction which could be improved later, and this goal was achieved.

Planning a perfectly functionable network before testing could be difficult, and it is important to shape and improve the network after appropriate testing.

Keywords/tags (subjects)

Infrastructure, network, planning, designing

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

1.1 Tehtävän kuvaus

Opinnäytetyönä pyrittiin kehittämään Caverion Suomi Oy:n elinkaarihankkeiden tietoverkkoratkaisuja parantaen näin talotekniikkaan liittyvien järjestelmien käytettävyyttä, toimintaa sekä varmuutta. Tutkimuksessa pyrittiin löytämään aiempien ratkaisuiden ongelmakohtia ja ratkaisut näihin suunnitelluissa tietoverkkomalleissa. Keskeinen tutkimuskysymys oli, voimmeko parantaa talotekniikkajärjestelmien toimintaa etsimällä tietoverkkojen ongelmakohtia sekä suunnittelemalla sellaiset tietoverkkosuunnitteluohjeet, joilla voidaan ratkaista nämä ongelmat?

1.2 Tutkimusmenetelmät

Tutkimuksen lähestymistapa on kvalitatiivinen. Tutkimuksessa pyrittiin ymmärtämään tutkittavaa ilmiötä syvällisemmin ja löytämään ratkaisuita ongelmakohtiin. Tietoverkon suunnittelussa ja mallintamisessa sekä sen ongelmien ratkaisemisessa käytettiin konstruktiivista tutkimusmenetelmää. Tutkimuksessa haastateltiin Caverion Suomi Oy:n eri osa-alueiden asiantuntijoita, ja pyrittiin poimimaan haastatteluista tietoverkoissa esiintyneitä ongelmakohtia sekä poimimaan hyviä neuvoja suunnitteluohjeeseen. Näin saatiin ymmärrystä laajennettua moneen eri näkökulmaan ja näkökulmia pyrittiin huomioimaan suunnitteluohjeessa.

1.3 Toimeksiantaja

Caverion Suomi Oy on kiinteistötekniikkaan suuntautunut yritys. Caverion suunnittelee, toteuttaa sekä ylläpitää monenlaisia ratkaisuita kiinteistöille sekä teollisuudelle. Caverionin liikevaihto vuonna 2018 oli noin 2,2 miljardia euroa ja on yksi Euroopan johtavia teknisiä ratkaisuita kiinteistöille ja teollisuudelle tarjoavia yhtiöitä. Caverionilla on noin 15 000 työntekijää 10 eri toimintamaassa. (Caverion lyhyesti 2019.)

2 Tietoverkko ja sen järjestelmiä

2.1 Uuden opetussuunnitelman mukainen ICT-tavoitearkkitehtuuri JHS179

2.1.1 Yleistä

JHS179 on suositus, jossa määritellään julkisen hallinnon kokonaisarkkitehtuurin yhtenäinen suunnittelumenetelmä, mukaan lukien yhtenäiset kuvaustavat ja kuvausmallit. Kokonaisarkkitehtuurilla tarkoitetaan tässä suosituksessa toiminnan, palvelujen, tietojen, erilaisten tietojärjestelmien sekä niiden tuottaman kokonaisuuden rakennetta. Suosituksen tarkoituksena on parantaa julkisen hallinnon toiminnan toimivuutta sekä parantaa palveluiden toimintaa sekä niiden yhteentoimivuutta. Tämä suositus on laaja ja käsittää siis koko kokonaisarkkitehtuurin kehittämisen ohjeita, mutta tietoverkon suunnittelussa tätä suositusta voidaan soveltaa hyvin sekä poimia suosituksesta oleelliset aiheet, jotka liittyvät tietoverkon suunnitteluun. Suositukseen liittyy neljä päänäkökulmaa: toiminta-, tieto-, tietojärjestelmä- sekä teknologia-arkkitehtuurinäkökulma. Suositus antaa hyvät ohjeet siitä, kuinka suunnittelua olisi hyvä viedä eteenpäin ja mitä asioita tulisi ottaa suunnittelussa huomioon. (JHS 179 Kokonaisarkkitehtuurin suunnittelu ja kehittäminen 2017, 3/77.)

2.1.2 Nykytilan selvittäminen

JHS179 mallia soveltaen projektissa on hyvä lähteä liikkeelle siitä, että kerätään tiedot nykytilasta sekä palveluista, eli tässä tapauksessa pyritään kartoittamaan mahdollisimman tarkasti nykyisten koulurakennusten tietoverkkoja ja niiden toimintaa ja palveluita. Neljästä esitellystä päänäkökulmasta tarkastellaan erityisesti kohtia, jotka koskettavat tietoverkkoa. Kartoitusta voidaan tehdä luomalla nykytilasta palvelukarttoja, palvelujen vuorovaikutuskarttoja ja tarkastelemalla verkkokuvia. Kuvataan loogisesti nykytilan tietomalleja sekä tietovirtoja. Pyritään selvittämään mahdollisimman perusteellisesti, miksi nykyiset toteutustavat on valittu. Tärkeänä osana tietoverkoissa on selvittää nykytilan teknologiapalvelut. Palvelut jaetaan eri osa-alueisiin eli eri teknologiadomaineihin ja tarkastellaan erityisesti niitä palveluita, jotka liittyvät

tietoverkkoon tai mitkä palvelut tulee ottaa tietoverkon suunnittelussa huomioon. Kun tarpeeksi tietoa nykytilasta on kerätty, kuvataan loogiset verkkokaaviot nykytilan tietoliikenneverkoista. Tietoverkkoja tulee tarkastella myös fyysisellä tasolla ja selvittää nykytilan palvelimet, laitteet, komponentit sekä fyysiset topologiat. Lopputuloksena nykytilan analysointivaiheen jälkeen saadaan hyvä pohjatietämys siitä, miten tietoverkkoja on suunniteltu jo valmistuneisiin rakennuksiin. (JHS 179 Kokonaisarkkitehtuurin suunnittelu ja kehittäminen 2017, 38-43/77.)

2.1.3 Tavoitetilan suunnittelu

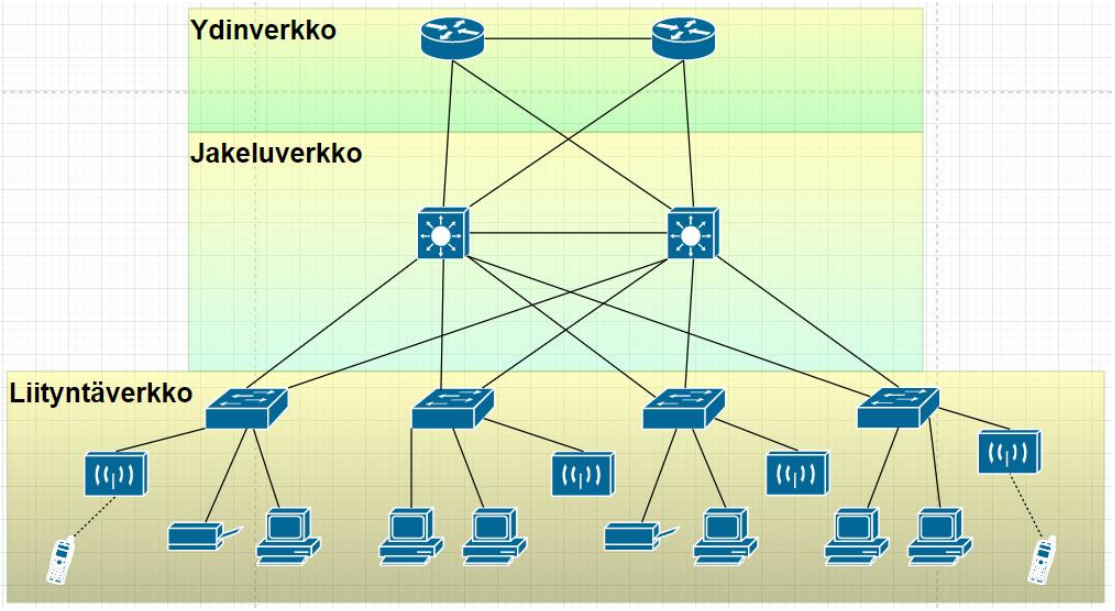
Tavoitetilan suunnittelu perustuu asetettuihin tavoitteisiin. Tavoitetilaan määritellään kehittämisperiaatteita nykytilan pohjalta. Tavoitteista muodostetaan kehittämisvaatimuksia. Määritellään tavoitetilan palvelukartta sekä palveluiden välinen suhdekartta. Kun tavoitetilan palvelut ovat selvillä, voidaan määritellä looginen malli kehitettävistä tietojärjestelmistä sekä niiden suhteista. Seuraavaksi määritellään aiempien pohjalta tavoitetilan teknologiavalinnat eli tekniikat, joilla tietojärjestelmät ja palvelut toteutetaan. Tietojärjestelmät voidaan sitten jakaa teknologiadomaineihin ja keskittyä niihin palveluihin ja järjestelmiin, jotka koskettavat tietoverkkoa. Palveluille on tärkeää myös huomioida tietoturvavaatimukset. Looginen verkkokaavio suunnitellaan tavoitetilan tietoliikenneverkosta ja palveluista, johon huomioidaan tietoturvallisuus. Näiden pohjalta suunnitellaan tavoitetilaa vastaavat ja palvelevat fyysiset verkkokuvat. Fyysisiin verkkokuviin kuvataan tarvittavat laitteet sekä palvelimet. Tavoitetilan lopputuloksena saadaan tavoitearkkitehtuurin kuvaus, josta löytyvät ratkaisut kehittämistarpeisiin. Tietoverkon näkökulmasta tavoitetilan suunnittelun jälkeen on jo hyvin selvillä, mitä tietoverkolta halutaan, jotta se vastaa tavoitetilan palveluita ja toiminnallisuutta sekä tietoturvallisuutta. (JHS 179 Kokonaisarkkitehtuurin suunnittelu ja kehittäminen 2017, 43-51/77.)

2.2 Erilaiset verkonsuunnittelumallit

Erikokoisille ja erityyppisille tietoverkoille on olemassa erilaisia suunnittelumalleja. Suunnittelumallin valinta riippuu usein verkon suuruudesta, kustannuksista sekä siitä, mitä verkolta halutaan.

2.2.1 Hierarkkinen verkkosuunnittelumalli

Kun suunnitellaan isompia verkkoja, kuten koulurakennusten verkkoratkaisuja, verkko kannattaa pilkkoa eri osa-alueisiin. Nämä osa-alueet ovat ydin- tai runkokerros, jakelukerros sekä liityntäkerros. Kyseiset verkot ovat hahmoteltuna kuviossa 1. Tämä on hierarkisen verkkosuunnittelun malli. Jokaisella kerroksella on oma tehtävänsä verkossa. Pilkkomalla verkko osiin yksinkertaistetaan verkon suunnittelua sekä saadaan helpommin valittua oikeanlaiset verkkolaitteet eri kerroksille vastaamaan verkon vaatimuksia. Hierarkinen malli on erittäin tehokas ja suosittu toteutustapa, joka maksimoi verkon suorituskyvyn ja skaalautuvuuden. (Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design 2014, 1.1.)



Kuvio 1. Kolmitasoinen, hierarkinen tietoverkkomalli

Liityntäkerroksen tehtävä on liittää päätelaite verkkoon sekä kuljettaa päätelaitteen liikenne eteenpäin jakelukerrokselle. Liityntäkerros koostuu yleensä Layer 2 -tason kytkimistä sekä langatonta verkkoa jakavista tukiasemista. Liityntäkerrokseen tulee enemmän verkkolaitteita kuin muille verkon kerroksille. Liityntäkerroksen tekniikoina

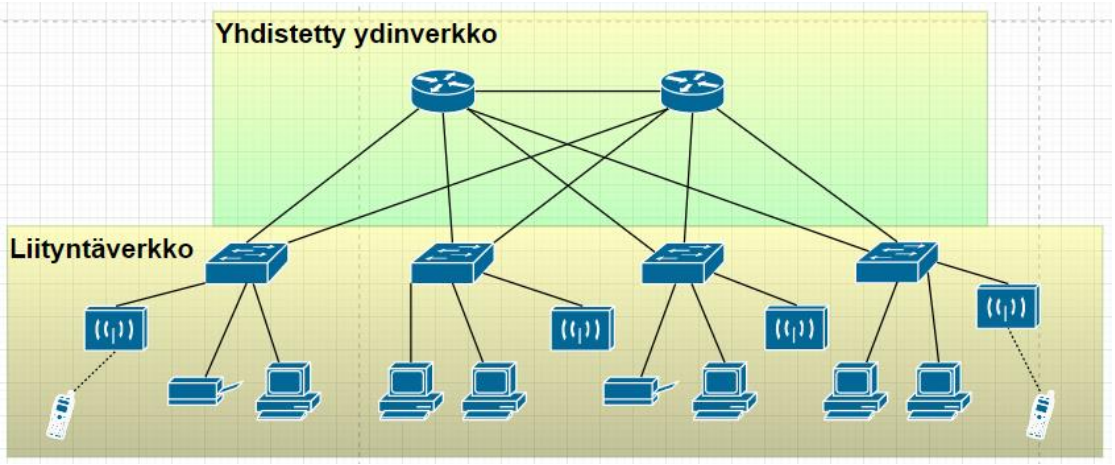
käytetään usein Ethernet -kaapelointia sekä langattomia tekniikoita. (Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design 2014, 1.1.2.2.)

Jakelukerros vastaanottaa sekä kokoaa yhteen liityntäkerroksen laitteiden liikenteen. Jakelukerroksen tehtävänä on kuljettaa liityntäkerroksen liikenne eteenpäin ydinkerrokselle, josta se reititetään päämäärään. Jakelukerroksella käytetään tehokkaampia sekä järeämpiä verkkolaitteita kuin liityntäkerroksella, sillä ne vastaanottavat huomattavasti enemmän dataa kuin esimerkiksi liityntäkerroksen kytkimet. Kaapelointeina voidaan käyttää kuitukaapelointia tai kuparikaapeleita. Jakelukerroksen laitteina voidaan käyttää esimerkiksi Layer 3 -tason kytkimiä, jolloin niillä voidaan myös parantaa verkon tietoturvaa sekä hallintaa hyödyntämällä pääsynhallintalistoja (ACL, Access Control List). Layer 3 -tason kytkimillä voidaan vähentää myös ydinkerroksen kuormaa, tuomalla verkon toiminnallisuutta kuten esimerkiksi DHCP palvelut lähemmäs päätelaitetta. Koska jakelukerros sisältää vähemmän laitteita ja koska niillä on erittäin tärkeä rooli verkossa, halutaan jakelukerrokselle usein enemmän luotettavuutta kuin esimerkiksi liityntäkerrokselle. Tämä saadaan kahdentamalla laitteet siten, että vaikka yksi jakelukerroksen kytkin vikaantuisi, liikenne saadaan silti kulkemaan toisten kytkimien kautta ydinkerrokselle. (Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design 2014, 1.1.2.3.)

Ydinkerroksella vastaanotetaan kaikki alemmilta kerroksilta saapuva liikenne sekä operaattorirajapinnasta tuleva liikenne, eli sen tulee välittää suuria määriä liikennettä nopeasti. Ydinkerroksen reitittimet käsittelevät suuren määrän dataa, joten laitteiden on oltava tarpeeksi tehokkaita vastaamaan verkon vaatimuksia. Myös ydinkerrokselle halutaan luotettavuutta ja vikasietoisuutta, eli usein ydinkerroksen laitteet on kahdennettu. Kaapelointina ydinkerroksella käytetään yleensä valokuitukaapeleita. Sillä ydinkerroksen laitteet ovat näistä kerroksista isoimman kuorman alla, on hyvä jos verkon toiminnallisuutta voidaan jakaa myös alemmille kerroksille. Sisäverkoissa usein nämä ydinkerroksen laitteet hoitavat palvelunlaadun (QoS, Quality Of Service), jolloin priorisoidaan tiettyjä liikenteitä toisenlaisen liikenteen edelle. (Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design 2014, 1.1.2.4.)

2.2.2 Kaksitasoinen verkkosuunnittelumalli

Hierarkkisessa suunnittelumallissa tietoverkko oli jaettu kolmeen erilaiseen kerrokseen. Kuitenkin ydin- ja jakeluverkko voidaan myös yhdistää. Mallia voidaan soveltaa tapauksissa, joissa verkko ei ole niin iso, tai tapauksissa, joissa tiedetään, että verkko ei tule enää kasvamaan sen elinkaaren aikana. Tässä mallissa puhutaan ”yhdistetystä rungosta” tarkoittaen sitä, että jakeluverkkoa ja runkoverkkoa ei rakenneta erikseen, vaan ne yhdistetään. Yhdistyneet verkot on hahmoteltuna kuviossa 2, jossa liityntäverkko pysyy entisellään. Tämä säästää verkon aktiivilaitteiden kustannuksissa, mutta esimerkiksi verkon skaalautuvuudesta verotetaan. (Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design 2014, 1.1.2.5.)



Kuvio 2. Kaksitasoinen, yhdistetty ydinverkko ja jakeluverkko

2.3 Tietoverkon saatavuus

Saatavuus on otettava tietoverkon suunnittelussa huomioon. Saatavuus kuvastaa sitä, kuinka paljon jokin palvelu tai yhteys on käytettävissä. Palvelut tai yhteydet eivät ole käytettävissä vikatilanteiden, huoltotöiden tai päivitysten takia. Kouluraken-

nuksen verkkoa suunnitellessa saatavuudessa otetaan huomioon ensisijaisesti vikatilanteet, sillä huoltotyöt tai päivitykset voidaan tehdä koulun aukioloaikojen ulkopuolella, jolloin alhaallaoloaika ei haittaa merkittävästi.

2.3.1 Saatavuuden määrittely

Tietoverkkoa suunniteltaessa on suunniteltava verkolle ja palveluille saatavuus. Kun jokin palvelu tai yhteys on saatavilla 99 % ajasta, voidaan palvelu silloin määritellä vikasietoiseksi. Kun saatavuusprosentti alkaa lähenemään 100 %, voidaan palvelua tai verkkoa kutsua jo korkeasti saatavaksi. Mitä lähemmäs 100 % mennään, sitä kalliimmaksi tietoverkon rakentaminen sekä ylläpito tulevat. Siksi on suunniteltava ja sovittava etukäteen, kuinka korkea saatavuustaso palveluilla tulee olla. Esimerkiksi jonkin ohjelmiston palveluntarjoajan palvelut tulee olla saatavissa 99.9999 % ajasta, mutta esimerkiksi yrityksen verkkosivujen vain noin 99.9 %. Näiden kahden välillä on jo huimat erot kustannuksissa sekä ylläpitovaatimuksissa. On siis mietittävä tarkasti suunnitteluvaiheessa, mikä saatavuustaso on tarpeellinen tarjottaville palveluille. (Planning for network availability n.d.)

2.3.2 Saatavuuden kartoitus

Saatavuus tulee kartoittaa suunniteltavalle verkolle palveluiden mukaisesti. Listataan siis palvelut tai sovellukset ja määritellään jokaiselle erikseen, kuinka saatavilla kyseinen palvelu tai sovellus tulisi olla. Loogisesta verkkokuvasta voidaan sitten tarkastella, mitä verkon eri osia tai laitteita sovellus tarvitsee toimiakseen, ja näin voidaan hahmotella palvelulle sen saatavuus. Loogisesta verkkokuvasta tarkastellaan siis yhteyden kulkua palvelulle tietoverkossa ja pyritään tunnistamaan riskitekijät liikenteelle. Riskitekijöitä ovat sellaiset solmukohdat verkossa, joita ei ole kahdennettu tai suunniteltu korvaavaa reittiä solmulle vikatilanteessa. Jos kahdentamaton solmukohta (Single Point Of Failure) vikaantuu, palvelu ei ole saatavilla. Palvelun saatavuus kasvaa, kun verkosta pyritään minimoimaan kaikki kahdentamattomat solmukohdat. Tietoverkosta listataan kaikki kahdentamattomat solmukohdat ja suunnitellaan kahdennussuunnitelma vastaamaan aiemmin luotua palveluiden saatavuuskartoitusta. Vikasietoisissa verkoissa kahdentamattomat solmukohdat ovat minimoitu. (Planning for network availability n.d.)

2.4 Kaapelityypit ja kaapelointi

2.4.1 Kuparikaapelit

Kuparikaapelit jaetaan erilaisiin kategorioihin, joilla on erilaisia vaatimuksia. Kaapelin on täytettävä vähintään kategorian mukaiset vaatimukset. Alle luokan 6 kaapeleita ei suositella enää käytettäväksi, sillä niiden hinta ei eroa paljoa korkeammista luokista ja niiden suorituskyky on paljon huonompi kuin korkeampien luokkien. Kuparikaapelikategorioiden ominaisuudet on summattu taulukkoon 1.

Taulukko 1. Kuparikaapelikategorioiden ominaisuudet

Kategoria	Taajuus	Luokka	Matka	Kaistanleveys
CAT 6	250 MHz	E	55 m	10 Gbit/s
CAT6A	500 MHz	E_A	100 m	10 Gbit/s
CAT7	600 MHz	F	100 m	10 Gbit/s

Kaapelit koostuvat kuparipareista. Kupariparit voivat saada elektromagneettista vuorovaikutusta, mikä aiheuttaa kaapelissa kulkevassa signaalissa virheilyä. Tältä pyritään välttymään suojaamalla kaapelin parit tai kaapelin ulkokuori. Suojaustapoja on erilaisia, ja kaapelin suojaus voidaan tunnistaa sen merkinnästä. Merkintä UTP (Unshielded Twisted Pair) tarkoittaa että kaapelia ei ole suojattu. Merkintä F/UTP (Outer Foiled, Inner Pairs Unshielded) tarkoittaa että kaapelin ulkokuori on suojattu foliolla, mutta sisällä kulkevia pareja ei ole erikseen suojattu. S/FTP (Outer Foil Shielded, Inner Pairs Foiled) merkintä tarkoittaa, että ulkokuori on suojattu foliolla, ja sisällä kulkevat parit on myös suojattu folioin. Jokainen pari on siis vielä erikseen kää-

ritty foliosuojukseen. Mitä paremmin kaapeli on suojattu, sitä vähemmän siihen aiheutuu elektromagneettista vuorovaikutusta. Kuitenkin suojaustaso vaikuttaa kaapelin hintaan, sekä sen taipuisuuteen. (10 Gbps Cabling n.d, 12-14; Flatman 2013, 10-13; IEEE Std 802.3an:2006, 135.)

2.4.2 Kuitukaapelit

Valokuitukaapelit voidaan jakaa karkeasti kahteen luokkaan: yksimuoto- sekä monimuotokuitukaapeleihin. Yksimuotokaapeleita kutsutaan etuliitteellä OS ja monimuotoa OM -liitteellä. Näille eri muotoluokille on kuitenkin vielä alaluokkia, mutta erona näiden kahden pääluokan välillä on se, että monimuotokaapelissa valo kulkee heijastumalla ja taittumalla kaapelissa, kun taas yksimuotokuidussa valo kulkee suoraan kaapelin päästä päähän. Monimuotokaapelin ydin on myös paksumpi kuin yksimuodon. Yksimuotokuidun aallonpituudet ovat tyypillisesti 1310 nm tai 1550 nm, kun taas monimuotokuidussa yleensä 850 nm tai 1300 nm. (McGrath & Bhaumik 2013.)

Yksimuotokuidut jaetaan kahteen alaluokkaan: OS1 sekä OS2 luokkiin. Yksimuotokuidussa esiintyy vähemmän vaimenemista kuin monimuodossa, mikä tarkoittaa sitä, että yksimuotokuidut soveltuvat paremmin pidemmän matkan yhteyksiin. Luokat OS1 ja OS2 eroavat eniten kaapelin rakenteeltaan. OS1 -kaapelit ovat tiukemmin rakennettuja, ja niissä sallitaan vaimennusta 1.0 dB/km. OS1 -kaapeleita käytetään usein rakennusten sisätiloissa. OS2 -kaapeli kulkee väljemmin suojakuoren sisällä, ja se soveltuu paremmin ulkokäyttöön, esimerkiksi maan alle. Kuitenkin OS2 -kaapelia voidaan käyttää yhtä hyvin myös rakennuksen sisällä, ja onkin nykyään yleisesti käytössä myös sisätiloissa. OS2 -kaapelin vaimennus on maksimissaan 0,4 dB/km. Mitä pienempi vaimennus kaapelissa, sitä pidempiin yhteyksiin se soveltuu. Yksimuotokuidut tarjoavat suuria tiedonsiirtokapasiteetteja pidemmälle matkalle kuin monimuotokuidut. (Difference Between OS1 and OS2 Single Mode Fiber Cable 2015; McGrath & Bhaumik 2013.)

Monimuotokuidut jaetaan myös alaluokkiin: OM1, OM2, OM3, OM4 ja OM5. Monimuotokuitujen suurempi ydin sallii sen, että kaapeleissa voidaan käyttää halvempia optiikoita kuten ledejä. Kuitenkin OM3 ja ylöspäin olevat luokat on optimoitu käyttämään laservaloa, jolloin saadaan enemmän tiedonsiirtonopeutta pidemmille matkoille. Kuitenkaan monimuotokuitukaapeleiden maksimietäisyydet eivät ole kovin suuria (10 Gbit/s alle 1 km), mikä tarkoittaa sitä, että monimuotokuitu sopii käytettäväksi erityisesti sisätiloissa, jossa etäisyydet ovat lyhyempiä. Monimuotokuitu on siis usein vaimennukseltaan, tiedonsiirtonopeudeltaan ja kantamaltaan huonompi vaihtoehto kuin yksimuotokuitu. (McGrath & Bhaumik 2013.)

2.5 Langaton verkko

2.5.1 Yleistä

Langaton verkko koostuu kahdesta päätaajuudesta: 2.4 Ghz sekä 5 Ghz. Näiden kahden taajuuden välillä on muutamia suuria eroja. Pienemmän taajuuden kantama on suurempi kuin isomman taajuuden. Pienemmät taajuudet myös läpäisevät paremmin esteitä, kuten seiniä. Kuitenkin pienemmät taajuudet tarjoavat hitaamman yhteyden kuin suuremmat taajuudet. Näin ollen 5 Ghz taajuuden kanavat ovat lähtökohtaisesti nopeampia, mutta niiden läpäisykyky sekä kantamat ovat pienempiä. Nämä kaksi päätaajuusaluetta sisältävät kanavia. Kuitenkin eri kanavat saattavat mennä päällekkäin, mikä aiheuttaa verkossa häiriöitä. 2.4 Ghz taajuus koostuu kanavista 1-13. Kuten taulukosta 2 huomataan, monet kanavista menevät taajuuksissa päällekkäin. Siksi suositellaan käytettäväksi sellaisia kanavia, jotka eivät mene päällekkäin missään tilanteessa. Nämä ovat 2.4 Ghz taajuudella kanavat 1, 6 ja 11. (Appendix A: Allowed Wi-Fi Channels n.d.; Channel Planning Best Practises n.d.)

Taulukko 2. 2.4 Ghz:n Wifi -kanavien taajuudet

Kanava	Alin taajuus (Mhz)	Ylin taajuus (Mhz)
1	2401	2423
2	2406	2428
3	2411	2433
4	2416	2438

5	2421	2443
6	2426	2448
7	2431	2453
8	2436	2458
9	2441	2463
10	2446	2468
11	2451	2473
12	2456	2478
13	2461	2483

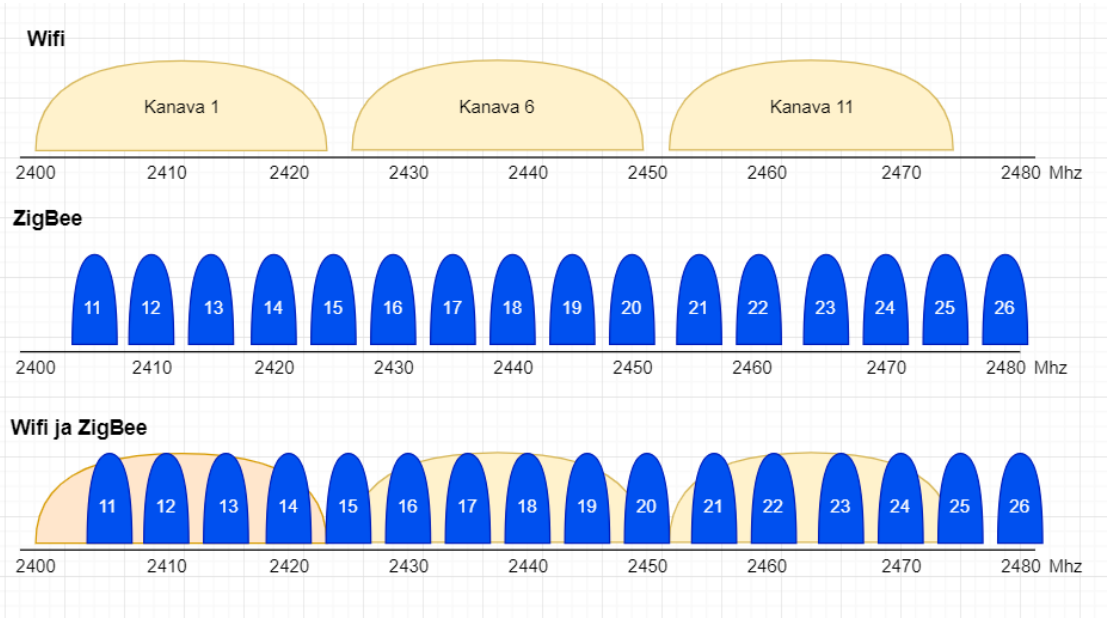
2.4 Ghz taajuuksia käyttää myös standardi 802.15.4. Tämän standardin taajuuksiin kuuluu myös ZigBee -taajuudet. Kanavien numeroinnit eroavat Wifi kanavista, mutta kanavien taajuudet osuvat kuitenkin päällekkäin, mikä voi aiheuttaa häiriöitä. ZigBee -kanavat eroavat Wifi -kanavista niiden leveydellä. Wifi -kanavat ovat jokainen 22Mhz leveitä, kun taas Zigbee vain 3Mhz. Siksi ZigBee -kanavat eivät mene päällekkäin toistensa kanssa, sillä kanavat ovat 5Mhz välein. ZigBee koostuu kanavista 11-26, joiden taajuudet esitellään taulukossa 3. (Channels, Zigbee 2018.)

Taulukko 3 ZigBee -kanavien taajuudet

Kanava	Taajuus (Mhz)
11	2405
12	2410
13	2415
14	2420
15	2425
16	2430
17	2435

18	2440
19	2445
20	2450
21	2455
22	2460
23	2465
24	2470
25	2475
26	2480

Kuviossa 3 huomataan, kuinka ZigBee -taajuudet osuvat Wifi -taajuuksien kanssa päällekkäin, vaikka kanavanumerot ovat erilaiset. Tästä syystä langattoman verkon suunnittelussa on oltava erityisen tarkkana käytettäessä molempia tekniikoita.



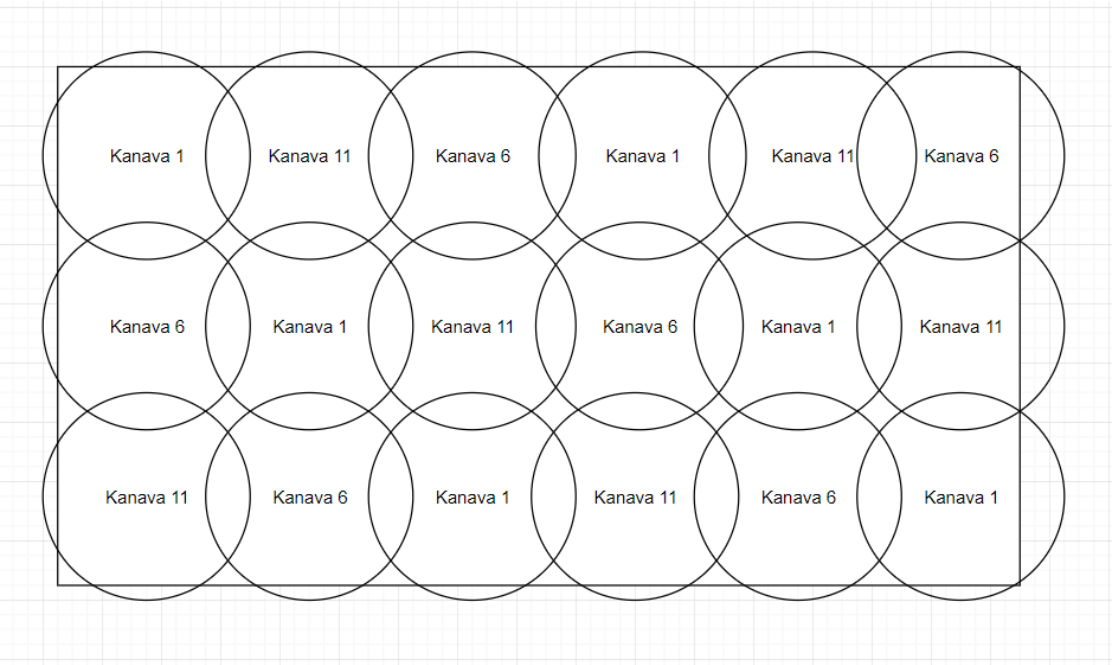
Kuvio 3 Wifi -kanavien ja ZigBee -kanavien päällekkäisyydet

2.5.2 Langattoman verkon häiriöt

Kun kaksi langattomassa verkossa olevaa laitetta lähettävät tai vastaanottavat dataa samaan aikaan samalla kanavalla, niiden signaalit törmäävät ja siten signaaliin syntyy häiriöitä ja mahdollisesti pakettihävikkiä. Jos yhteentörmäyksiä samalla taajuudella tulee liikaa, langattomasta verkosta tulee käyttökelvoton pakettihäviön vuoksi. Siksi 802.11 -standardien mukaiset laitteet käyttävät langattomassa verkossa vapaan kanavan tarkistustekniikkaa, jota kutsutaan nimellä CCA (Clear Channel Assessment). Tämä tarkoittaa sitä, että ennen kuin laite alkaa lähettää vastaanottimelle omaa dataansa, se kuuntelee langattoman verkon kanavaa ja sitä, lähettääkö joku muu samaan aikaan kanavalla. Jos kanava on vapaa, laite voi lähettää oman datansa tukiasemalle. Jos kanavalla joku muu lähettää CCA tarkistuksen aikana, laite odottaa omaa vuoroaan lähetykselle, eikä lähetä kanavalle päällekkäin. Tämä tekniikka välttää datan yhteentörmäystä samalla kanavalla. Kuitenkaan tämä tekniikka ei välttämättä huomaa, jos joku lähettää samaan aikaa eri kanavalla mutta samalla taajuudella, sillä kanavissa on taajuuspäällekkäisyyksiä. Tästä syystä CCA tarkistus ei voi korjata kaikkia virheitä langattomassa verkossa, siksi taajuuksien suunnittelu on erittäin tärkeää hyvän lopputuloksen saamiseksi. (Channel Planning Best Practises n.d.)

2.5.3 2.4 Ghz:n kanavasuunnittelu

Langattomassa verkossa halutaan eri kanavien päällekkäisyyksiä, jotta peittoalue signaalille saadaan jokaiseen paikkaan. Jos eri kanavat eivät mene ollenkaan päällekkäin, niiden väliin syntyy katvealue, jossa signaalia ei ole. Kuten aiemmassa kappaleessa todettiin, kuitenkaan emme halua suunnitella päällekkäisyyksiä kanaville, jotka käyttävät samoja taajuuksia. Siksi langaton verkko suunnitellaan käyttäen kanavia 1, 6 sekä 11 siten, että ne menevät hieman päällekkäin. Kuviossa 4 on hahmoteltu, kuinka tukiasemat voisi sijoitella kuvitteelliseen rakennukseen siten, että signaalit menevät päällekkäin, mutta kuitenkin siten että samat kanavat eivät ole päällekkäin toistensa kanssa. (Appendix A: Allowed Wi-Fi Channels n.d.; Channel Planning Best Practises n.d.)



Kuvio 4. 2.4 Ghz kanavien suunnittelumalli

2.5.4 5 Ghz:n taajuudet

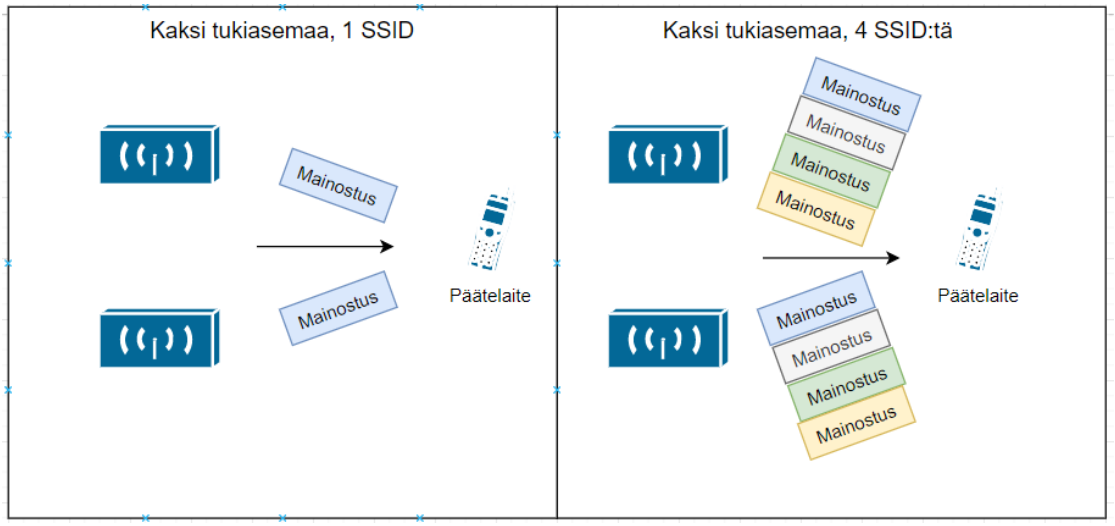
5 Ghz:n taajuudet jaetaan kolmeen erilaiseen UNII (Unlicensed National Information Infrastructure) -luokkaan, jotka ovat UNII-1, UNII-2, sekä UNII-3. Nämä kaikki luokat sisältävät eri taajuuksia. 5 Ghz:n kanavat jaetaan joka neljänteen eli päällekkäisyyksiä ei synny, kuten 2.4 Ghz:n kanavissa. UNII-1 sisältää kanavat 36, 40, 44 sekä 48. UNII-2 luokka sisältää kanavat 52, 56, 60, 64 sekä laajennetun version 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, sekä 140. UNII-3 sisältää kanavat 149, 153, 157 ja 161. Kanavia on siis huomattavasti enemmän käytössä kuin 2.4 Ghz:n tekniikassa. Kuitenkin nämä kanavat sisältävät rajoituksia, kuten sen että Euroopassa kanavia 36-64 saa käyttää ainoastaan sisätiloissa, sekä kanavilla 52-140 on käytettävä DFS (Dynamic Frequency Selection) -tekniikkaa. DFS -tekniikka estää häiriöitä tutkissa, joka tarkoittaa sitä, että jos tukiasema havaitsee tutkasignaalin, on sen välittömästi vaihdettava kanavaa. Kuitenkin käytettävissä olevat kanavat voidaan hyödyntää siten, että signaali kattaa jokaisen alueen eikä samat taajuudet mene päällekkäin. Alustava kana-

vasuunnittelu voidaan toteuttaa samalla tavalla kuin 2.4 Ghz:n taajuuksilla, piirtämällä karkeasti rakennukseen eri kanavat ja niiden peittoalueet. (Appendix A: Allowed Wi-Fi Channels n.d.; Channel Planning Best Practises n.d.)

2.5.5 Monen SSID:n toteutus

Langattomaan verkkoon voi syntyä häiriöitä, jos kaksi laitetta juttelee samaan aikaan samalla taajuudella. Häiriöitä saattaa aiheutua vaikka langaton verkko (SSID) olisi eri, mutta taajuus sama. Jos jaamme yhdellä tukiasemalla useampaa SSID:tä, voimme ajatella, että jokainen SSID on oma virtuaalinen tukiasemansa, joka toimii samalla tavoin kuin fyysinen tukiasema. Jokainen virtuaalinen tukiasema käyttää fyysisen tukiaseman taajuuksia. Tämä tarkoittaa sitä, että useamman SSID:n jakaminen yhdellä fyysisellä tukiasemalla on lähes sama kuin se jos fyysisiä tukiasemia olisi useita, joista jokainen jakaisi omaa verkkoaan. Useat SSID:t myös ruuhkauttavat verkkoa.

Voidaan ajatella esimerkkinä langattoman verkon hallintaliikennettä. Hallintaliikenne koostuu jokaisen virtuaalisen tukiaseman lähettämistä paketeista, joilla se mainostaa verkkoaan. Päätelaitteet lähettävät myös paketteja etsiessään vapaita langattomia verkkoja, joihin kaikki virtuaaliset tukiasemat vastaavat. Esimerkiksi jos kaksi fyysistä tukiasemaa toimivat samalla kanavalla, ja jakavat samaa SSID:tä, molemmat niistä lähettävät mainostuspaketteja, sekä molemmat vastaavat päätelaitteiden kyselyihin. Jos nämä kaksi tukiasemaa jakaisivat esim. neljää eri SSID:tä, mainostuspaketteja tulisi kahdeksalta eri virtuaaliselta tukiasemalta, ja päätelaitteen etsiessä verkkoa, se saa vastauksen kahdeksalta eri virtuaaliselta tukiasemalta. Tämä tarkoittaa siis sitä, että hallintaliikenteestä syntyy paljon enemmän kuormaa verkolle SSID:iden määrän kasvaessa, esimerkin tilanne nähdään kuviossa 5. Siksi on harkittava tarkkaan, mitä langattomia verkkoja tarvitaan ja millä taajuuksilla ne toimivat. Yleensä syy monen verkon jakamiselle on se, että eri verkoille halutaan erilaisia salauksia ja oikeuksia. Yhdellä fyysisellä tukiasemalla ei suositella jaettavaksi yli kolmea langatonta verkkoa. (Multi-SSID Deployment Considerations n.d.)



Kuvio 5. Monen SSID:n aiheuttama kuorma

2.6 Turvajärjestelmät (Lenel)

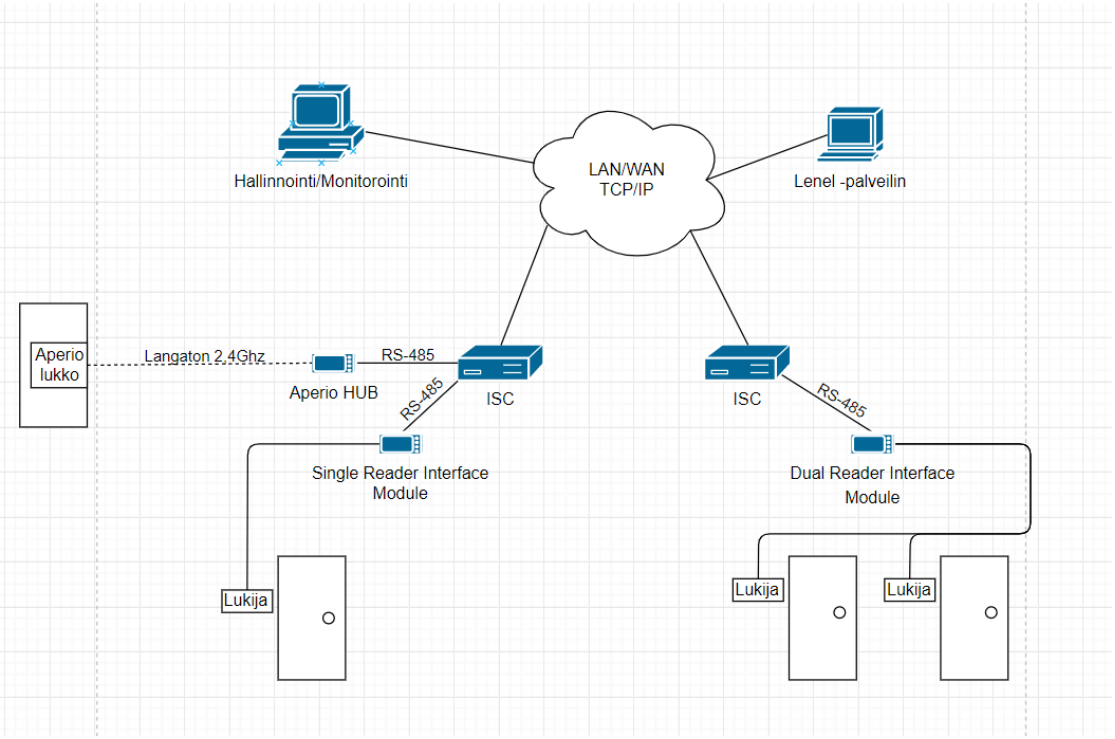
2.6.1 Yleistä

Lenel on maailmanlaajuisesti johtavassa asemassa edistyneissä turvallisuusjärjestelmissä. Lenel tuottaa innovatiivisia ratkaisuita rakennusten sekä ihmisten suojaamiseen. Lenelin yrityssovellukset hallinnoivat monia erilaisia turvajärjestelmiä tarjoamaan yhden, toimivan turvallisuusratkaisun tilaajalle. Lenel järjestelmällä voidaan toteuttaa esimerkiksi kulunvalvonta- sekä hallintajärjestelmiä, rikosilmoitusjärjestelmiä, paloilmoitinjärjestelmiä, kameravalvonta- tai tunnistusjärjestelmiä sekä paljon muuta. (News & Events 2018.)

2.6.2 Toimintaperiaate

Lenel -palvelin päivittää sekä lukee tietokantaa, jossa data säilötään. Lenel -palvelin juttelee kontrollereiden (ISC, Intelligent System Controller) kanssa, joille se kertoo pääsyoikeusmuutoksista. Kontrollereilla on siis aina tieto siitä, kellä on oikeus avata

esimerkiksi sen käskyttämiä lukkoja. Kontrollerit juttelevat Lenel -palvelimen suuntaan kertoen tapahtumista, esimerkiksi lukon avauksesta. Lenel palvelinohjelmisto voidaan ajaa virtuaalipalvelimilla, jolloin voidaan käyttää palvelimien klusterointi sekä Failover menetelmiä. Näin saadaan Lenel -palvelimesta erittäin vikasietoinen. Kontrollerit voivat jutella Lenel -palvelinohjelmiston kanssa kahdennetun Ethernetin ylitse. Kontrollereissa on myös omaa muistia, tarkoittaen sitä että jos kommukaatio vikatilanteen vuoksi Lenel -palvelimelle katkeaa, kontrolleri pystyy silti toimimaan määritellyllä tavalla, aukaisten esimerkiksi ovien lukkoja muistiin tallennettujen oikeuksien avulla sekä pitämään muistissaan 50 000 tapahtumaa, jotka se kertoo myös palvelimelle yhteyden palautuessa. Yhteyden palautuessa palvelin synkronoi pääsyoikeuspäivitykset kontrollerin kanssa. Kontrollereihin yhdistetään lukija moduuleita (Reader Interface Module), joihin liitetään varsinaiset lukijalaitteet. Moduuleita on erilaisia, yhden- sekä useamman lukijan malleja, myös langattomia versioita, kuten ASSA ABLOY Aperio lukot. Langattomia lukkoja varten kytketään ISC kontrolleriin Aperio Hubeja, jotka juttelevat langattomasti lukon kanssa. Hub juttelee kontrollerin kanssa RS-485 -standardin mukaisesti. Myös langalliset moduulit juttelevat kontrollerin kanssa RS-485 -standardin mukaisesti, käyttäen protokollina mm. OSDP protokollaa, tai OSDP Secure Channel protokollaa, joka on salattu AES128 salauksella. Kontrollereiden ja Lenel -palvelimen välinen liikenne voidaan suojata TLS1.2 salauksella. Lenel -järjestelmän toimintaa on hahmoteltu kuviossa 6. (LNL-3300, 2017; LNL-X4420, 2018; LNL-1300 Series 2, 2014; Access, 2015; Assa Abloy Aperio Locks, 2014; Aperio™ AH30 -keskitin jopa 8 langattomalle ovelle n.d.)



Kuvio 6. Lenel -järjestelmäkaavioesimerkki

Lenelin viimeisin OnGuard 7.5 versio tarjoaa paljon uusia ominaisuuksia järjestelmälle. OnGuard ohjelmistoa voidaan hallita selaimen kautta etänä myös matkapuhelimilla, ja sen tietoturvallisuutta on parannettu aiemmista versioista. OnGuard 7.5 -järjestelmällä voidaan esimerkiksi katsella selaimen kautta kameroiden tuottamaa live kuvaa perustuen järjestelmän antamiin tapahtumiin. (OnGuard Version 7.5 2018.)

2.6.3 Tietoverkon vaatimukset

Tietoverkon suunnittelussa on otettava huomioon Lenel -järjestelmän vaatimukset. Järjestelmä sisältää IP liikennettä palvelimen sekä kontrollereiden välillä. Myös monitorointi- sekä hallinnointityöasemat liittyvät IP verkkoon. Kontrollereiden sekä palvelimen välinen liikenne on pientä, mutta tärkeää. Jos IP kameravalvonta toteutetaan

Lenel -järjestelmällä, kamerat liittyvät Lenel NVR (Network Video Recorder) tallentimelle IP verkon kautta. Kameroiden videoliikenteestä aiheutuu tietoverkolle enemmän kuormaa, joka on otettava kapasiteettilaskennassa huomioon. Kameraverkko suositellaan toteutettavaksi tietoturvasyistä erillisenä virtuaalisena lähiverkkona, jonne on rajoitetut oikeudet. (Access 2015.)

Jos järjestelmässä käytetään langattomia ASSA ABLOY Aperio -lukkoja, on otettava erityisesti huomioon radiohäiriöt. ASSA ABLOY Aperio -järjestelmä toimii Hubilla joka liitetään ISC kontrolleriin sekä lukoilla, jotka juttelevat langattomasti 2.4 Ghz (IEEE 802.15.4) taajuudella Hubin kanssa. Hubin sekä lukon välinen kommunikaatioetäisyys on noin 20 metriä jos häiriöitä ei ole. Hubi sekä lukot voivat käyttää kanavia 11-26, eli ne käyttävät ZigBee taajuuksia, johon sisältyy yhteensä 16 kanavaa. Langaton radioliikenne salataan AES128 salausmenetelmällä. Hubien ja rakennuksessa olevien tukiasemien sijainnit on suunniteltava siten, että kaistojen päällekkäisyyksiä tulisi mahdollisimman vähän. (Aperio™ AH30 -keskitin jopa 8 langattomalle ovelle n.d.)

2.7 Valaistusjärjestelmät (Dali, Helvar)

2.7.1 Yleistä

DALI (Digital Addressable Lighting Interface) on standardissa IEC 62386 määritelty protokolla, jolla valaisimet voivat jutella digitaalisesti toisilleen käyttäen komponenteilla olevia osoitteita. Helvar on DALI standardin johtava kehittäjä, ja tarjoaa todella monia erilaisia hallintalaitteita sekä rajapintoja DALI -järjestelmälle. Helvarin Imagine -valaistuksen hallintaratkaisu on suunniteltu suurienkin valaistusratkaisuiden hallintaan, ja se voidaan integroida myös muihin kiinteistöautomaatiojärjestelmiin liittämällä DALI -järjestelmä Ethernet verkkoon hyödyntäen Helvarin tarjoamia reitittimiä. (DALI - Digital Addressable Lighting Interface 2019; Imagine 2019.)

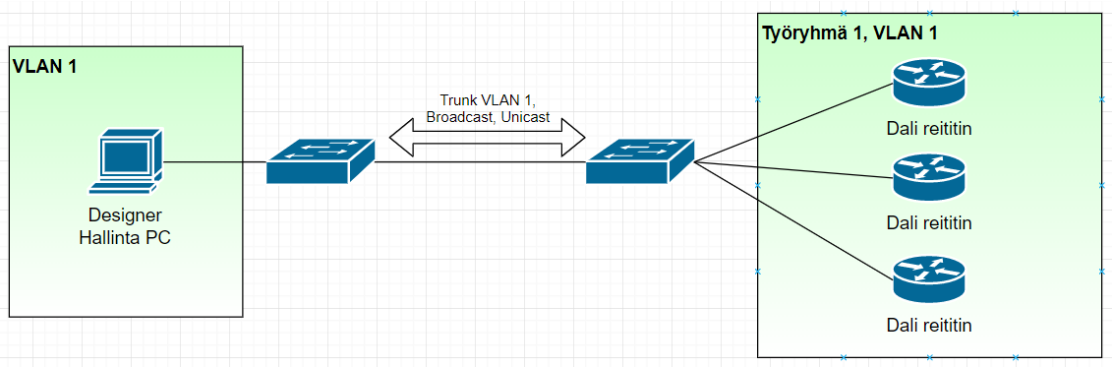
2.7.2 Toimintaperiaate

DALI -järjestelmällä hallitaan valaistusta, ja se voidaan liittää kiinteistöautomaatio järjestelmiin, tai se voi toimia täysin itsenäisesti. Helvar Imagine järjestelmä koostuu

monista erilaisista komponenteista, joilla voi räätälöidä valaistusjärjestelmän vastaamaan monenlaisia tarpeita. Järjestelmään kuuluu esimerkiksi erilaisia järjestelmäsensoreita, jotka voivat ohjailla valaisimia automaattisesti, säätimiä, jotka säätelevät valaisimia sekä releyksiköitä, joilla voidaan ohjailla erilaisia ei-valaisimia, esimerkiksi verhoja. Sisäänmenoyksiköillä voidaan liittää valonohjausjärjestelmään ulkoisia kytkimiä, ajastimia tai sensoreita. Nämä DALI -järjestelmän komponentit liitetään reitittimiin. Helvar 920 ja 910 sarjan reitittimillä voidaan yhdellä reitittimellä liittää järjestelmään 128 DALI -järjestelmän laitetta. Reitittimissä on kaksi DALI väylää, joista kumpaankin voidaan yhdistää 64 laitetta. DALI reitittimet liittyvät sitten yleiskaapelointiverkkoon Ethernet yhteydellä, mahdollistaen esimerkiksi järjestelmän hallinnan graafiselta käyttöliittymältä, tai integraation muihin kiinteistöautomaatiojärjestelmiin. Järjestelmään kuuluu olennaisesti myös hallintaohjelmistot. Designer -ohjelmistolla voidaan ohjelmoida, konfiguroida sekä käyttöönottaa reititinjärjestelmiä. Designer ohjelmistolla myös ylläpidetään reititinjärjestelmää, eli se on hyvin olennainen komponentti reititinjärjestelmässä. Designer ohjelmiston käyttöön kuitenkin tarvitsee Helvarin oman koulutuksen, josta saa sertifioinnin reititinjärjestelmien käyttöönottoon. (Kupari 2018; Murtoniemi 2018; Tuotteet 2019.)

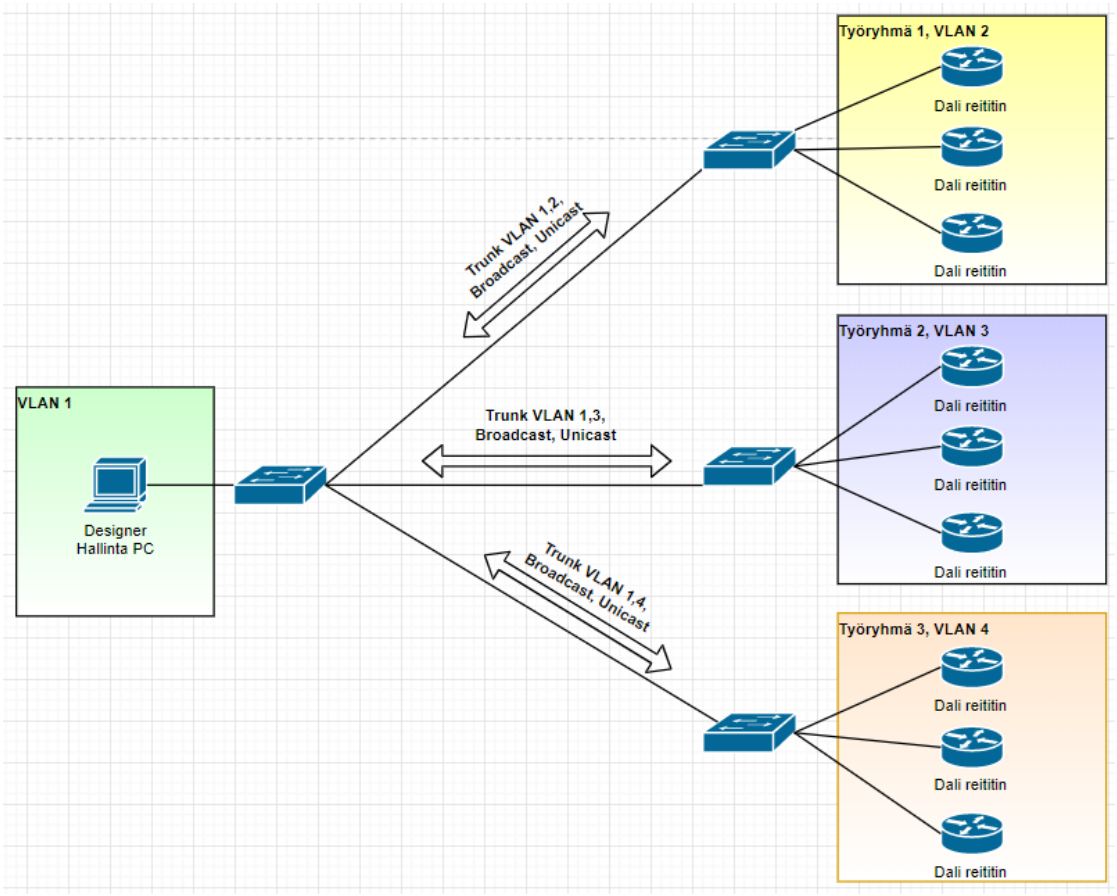
2.7.3 Tietoverkon vaatimukset

Reitittimet jaetaan työryhmiin. Työryhmät tarkoittavat tässä tapauksessa virtuaalista aliverkkoa, eli VLAN:ia. Reitittimien jaossa tulee ottaa huomioon verkon koko. On suositeltavaa, että suuremmissa järjestelmissä (n. yli 30 reititintä) jaetaan reitittimet useampaan työryhmään (Multi-Cluster). Työryhmäjako voidaan tehdä esimerkiksi kerroksen tai rakennuksen perusteella. Pienemmissä verkoissa riittää yksi työryhmä (Single Cluster), johon kaikki reitittimet yhdistetään. Tietokoneella, johon on asennettuna Designer hallinta ohjelmisto, täytyy olla yhteys kaikkiin työryhmiin sekä kaikkiin reitittimiin. Jos työryhmiä on useita, työryhmien ei tarvitse liikennöidä keskenään, mutta työryhmien sisällä reitittimien on voitava liikennöidä keskenään. Broadcast ja Unicast -liikenteet on oltava nähtävillä siis saman VLANin sisällä kaikille reitittimille, ja Unicast- ja Broadcastliikenteen on oltava näkyvillä jokaisesta VLANista Desinger -tietokoneelle. Kuviossa 7 on hahmoteltuna pienempi yhden työryhmän toteutus. (Kupari 2018; Murtoniemi 2018; 910 Router 2019; 920 Router 2019.)



Kuvio 7. Pienempi, yhden työryhmän toteutus

Kuitenkin isommissa, yli kolmenkymmenen reitittimen verkoissa on suositeltavaa jakaa reitittimet useampaan työryhmään. Monen työryhmän toteutus on hahmoteltuna kuvioon 8. (Murtoniemi 2018.)



Kuvio 8. Suurempi, monen työryhmän toteutus

Monen työryhmän toteutuksessa on tärkeää huomioida, että eri työryhmistä Broadcast- sekä Unicastliikenteen on kuljettava Designer -hallinta PC:n VLANiin, joka ei onnistu ilman Bridge-Groupin konfigurointia. Siksi pienemmissä toteutuksissa on yksinkertaisempaa käyttää yhden työryhmän VLAN -mallia. (Bridging Traffic n.d, 3-5; Chapter: Configuring Bridged Mode 2018.)

2.8 Audiovisuaaliset järjestelmät (Wolfvision Cynap)

2.8.1 Yleistä

Wolfvisionin kehittämä Cynap -järjestelmä on langaton vuorovaikutus- sekä esitysjärjestelmä. Järjestelmä sisältää sisäänrakennetun mediasoittimen, mahdollisuuden

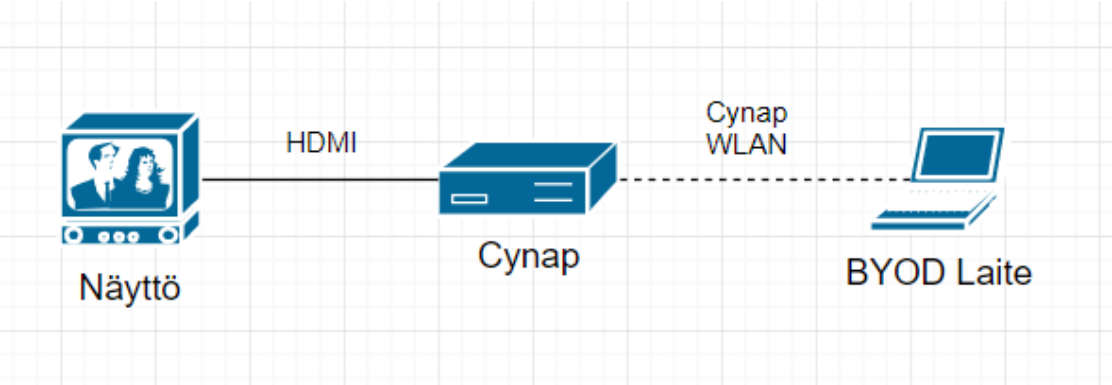
web kokouksille, nauhoitusta sekä jakamista, streamausta, tuen näyttöjen ja sisällön jakamiselle BYOD (Bring Your Own Device) laitteilta sekä paljon muuta. Cynap -järjestelmää käytetään siis esimerkiksi kokoushuoneissa tai oppimisympäristöissä, koska sillä voidaan helposti yhdistää sisältö ja dynaaminen informaation jakaminen kaikkien osallistujien välillä. Cynap -järjestelmällä voidaan siis luoda isostakin tilasta täysin aktiivinen oppimisympäristö. Cynap -järjestelmä voidaan yhdistää olemassa olevaan tietoverkkoinfrastruktuuriin, jolloin yhteydet kulkevat sen kautta. Cynap voi liittyä verkkoon langattomasti ja BYOD laitteet voivat yhdistyä Cynap -järjestelmään langattomasti. Cynap -järjestelmän laitteisto ja niiden ominaisuudet on kuvattu taulukossa 4. (High Performance Collaboration 2019.)

Taulukko 4 Cynap -järjestelmän laitteiston ominaisuudet

Laite	Cynap	Cynap Core	Cynap Pure
Ominaisuudet	Keskuslaite, palvelee 40 Cynap Corea. Saatavilla Cynap Matrix -sovellus	Näytön yhteyteen tuleva laite, tukee matriisi -ominaisuutta	Tarkoitettu yhdelle näytölle langatonta kuvansiirtoa varten, ei tue matriisia

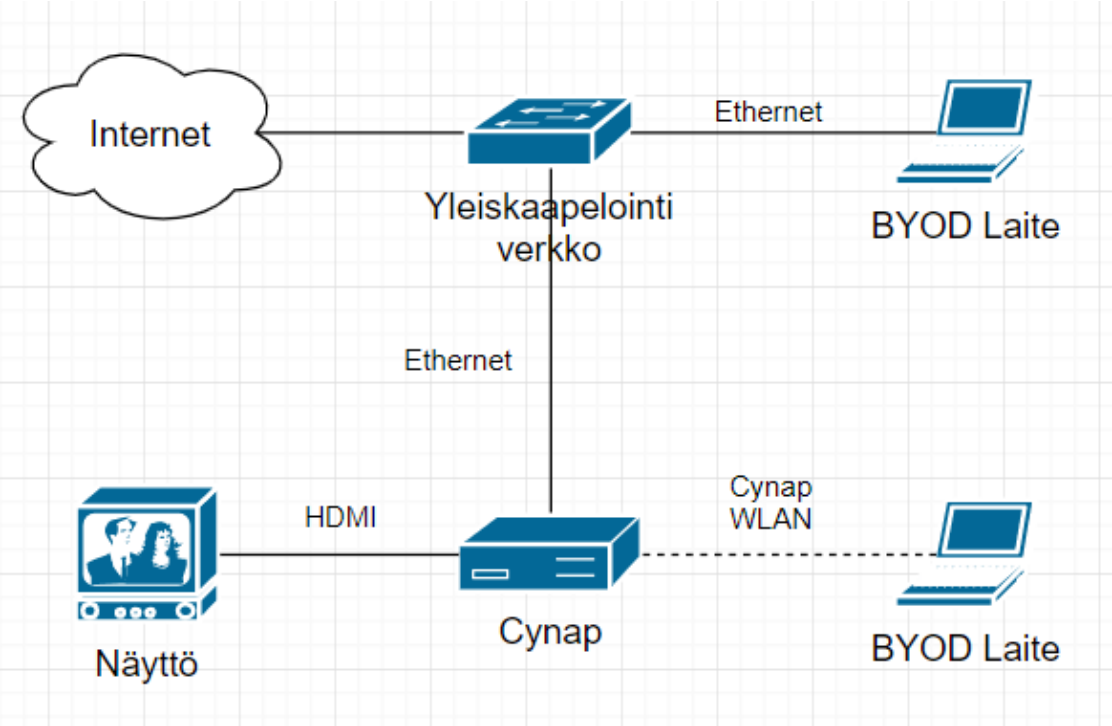
2.8.2 Toimintaperiaate

Cynap -järjestelmä kokonaisuudessaan koostuu muutamasta komponentista. Järjestelmä koostuu Cynap -laitteista, näytöistä, BYOD laitteista sekä olemassa olevasta tietoverkosta. Cynap -järjestelmää voidaan käyttää muutamalla eri tavalla. Cynap voi olla myös täysin itsenäinen järjestelmänsä. Tässä konfiguraatiossa Cynap jakaa itse langatonta verkkoa, johon BYOD laitteet liittyvät. Sitten BYOD laitteet voivat jakaa verkosta sisältöä, joka nähdään Cynap -laitteeseen liitetyllä näyttöpäätteellä. Tässä konfiguraatiossa laitteet eivät kuitenkaan pääse Cynap -verkosta internettiin, eikä Cynap pääse käsiksi esimerkiksi pilvipalveluihin tai internet sisältöön, sillä sitä ei kytketä verkkoon. Itsenäisen järjestelmän konfiguraatio esitellään kuviossa 9. (Theiner 2018, 9.)



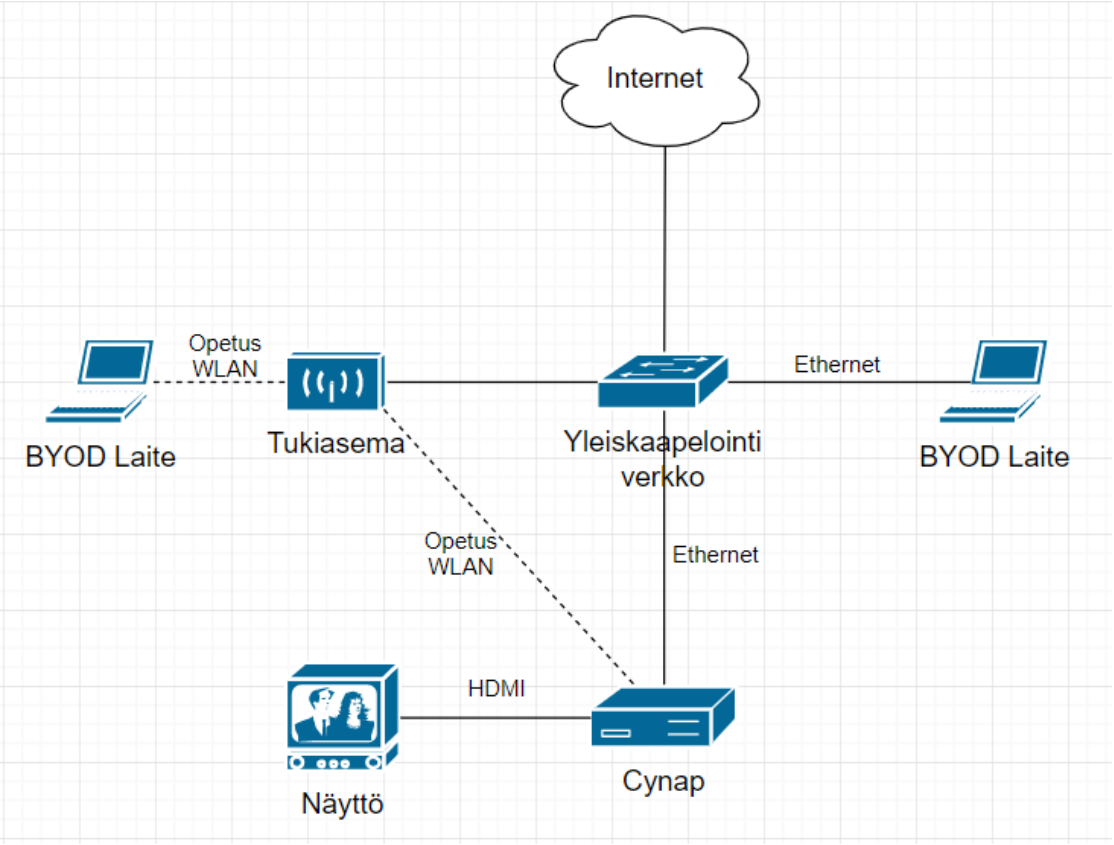
Kuvio 9. Cynap itsenäisenä järjestelmänä

Jos Cynapia käytetään itsenäisenä järjestelmänä, ei koskaan päästä hyödyntämään kaikkia sen ominaisuuksia. Toinen tapa käyttää Cynap -järjestelmää on liittää se talon yleiskaapelointiverkkoon sekä internettiin. Tässä konfiguraatiossa Cynap pääsee internettiin, jolloin se pääsee näkemään paljon enemmän sisältöä sekä pilvipalveluiden resursseja voidaan hyödyntää. Cynap saa myös tarkistettua verkosta järjestelmäpäivityksensä. Toinen konfiguraatiotapa näkyy kuviosta 10. Tässä konfiguraatiossa Cynap WLANista ei kuitenkaan pääse internettiin, vaikka Cynap on liitettynä verkkoon. Cynap ei toimi reitittimenä tai gatewayna laitteille. Tässä konfiguraatiossa samassa aliverkossa olevat laitteet voivat yhdistyä Cynap -laitteeseen tietoverkon kautta. (Theiner 2018, 10.)



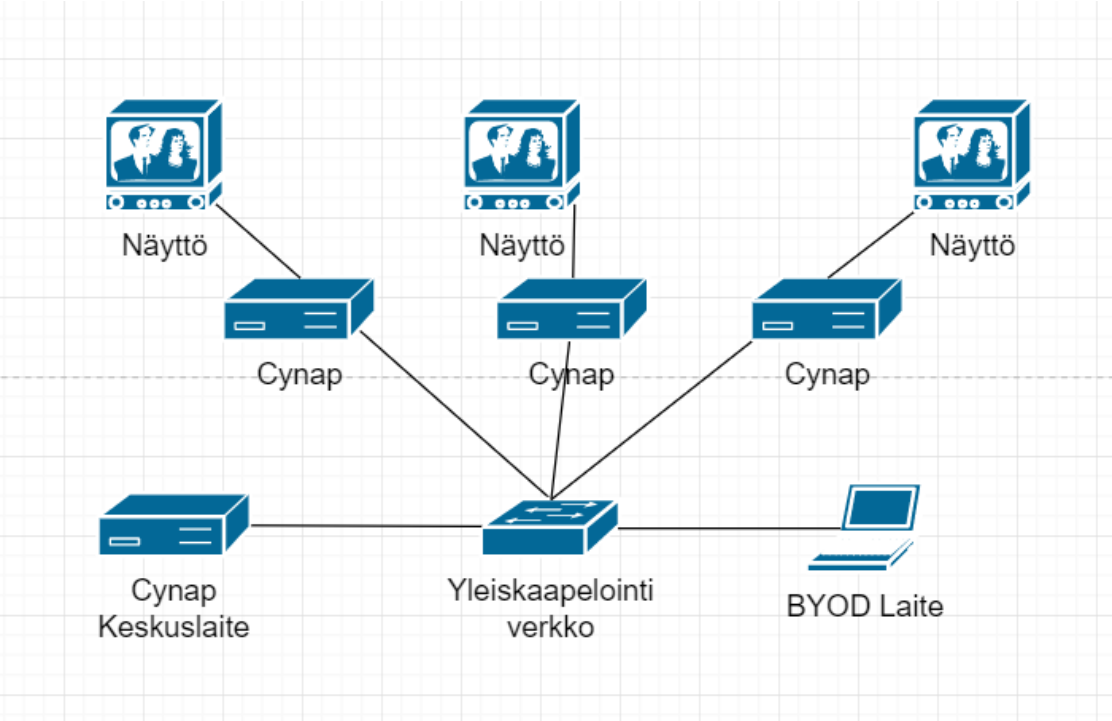
Kuvio 10. Cynap liitettynä yleiskaapelointiverkkoon

Kolmannessa konfiguraatiossa esitetään, kuinka Cynap toimii ”Infrastructure” tilassa. Tässä konfiguraatiossa Cynap ei enää jaa omaa WLAN -verkkoaan, vaan se liitetään osaksi olemassa olemaa langatonta verkkoa, johon myös BYOD laitteet liittyvät. Näin ollen BYOD laitteet eivät ole millään tavalla riippuvaisia Cynap -laitteen läheisyydestä. Cynap on siis liitettynä piuhalla yleiskaapelointiverkkoon (voi olla eri aliverkko) sekä langattomasti esimerkiksi opetusverkkoon. Näin kaikki BYOD laitteet opetusverkosta sekä yleiskaapeloinnin aliverkosta voivat yhdistyä Cynap -järjestelmään. Tämä konfiguraatio esitellään kuviossa 11. (Theiner 2018, 11.)



Kuvio 11. Cynap "Infrastructure" -konfiguraatiossa

Kuitenkin jos Cynap laitteita on useita ja halutaan niiden esimerkiksi toistavan samaa sisältöä ja toimivan yhdessä, tarvitaan keskuslaite. Keskuslaite muodostaa matriisin, joka yhdistää Cynap laitteet. Keskuslaite hallitsee matriisissa olevia Cynap laitteita, ja voi esimerkiksi toistaa yhtä streamia viidellä Cynap -laitteella ja toista streamia muilla. Tekniikkaa kutsutaan vSolution Matrix tekniikaksi, eli tietoverkkopohjaiseksi AV järjestelmäksi. Yhteen keskuslaitteeseen voi liittää maksimissaan 40 Cynap, tai Cynap Core -laitetta. Kuviossa 12 nähdään keskuslaite, joka ohjailee kolmea Cynap laitetta. (vSolution MATRIX 2019.)



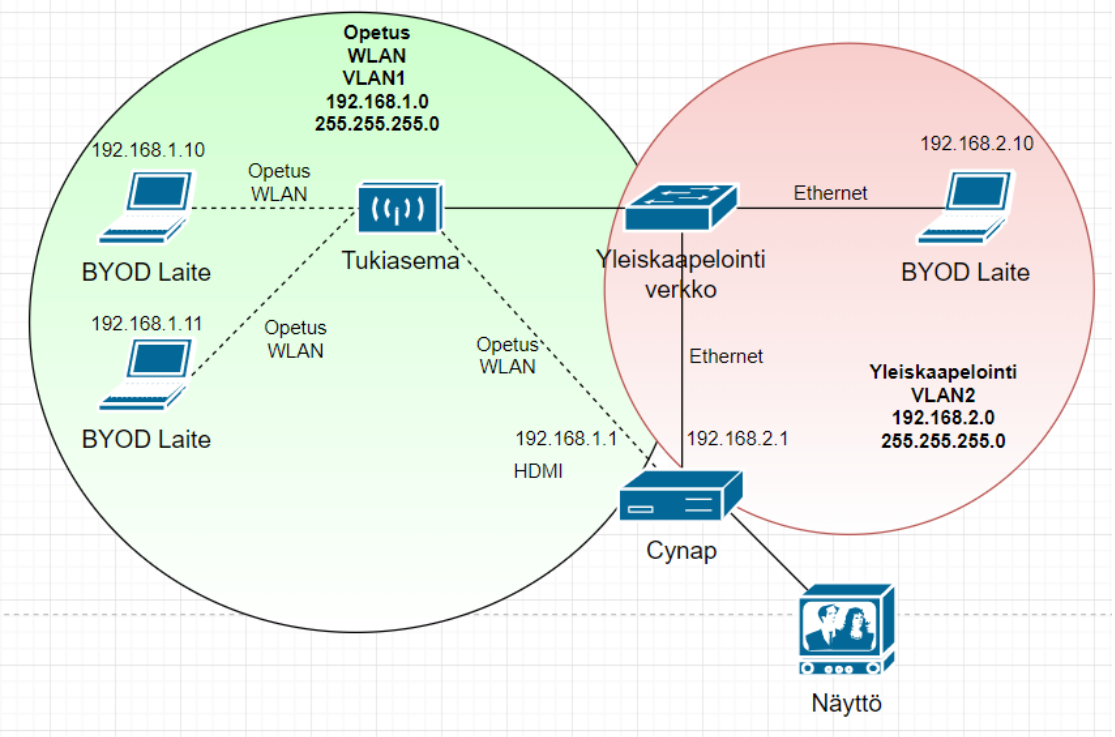
Kuvio 12 vSoltion Matrix -tekniikalla yhdistetyt Cynap -laitteet

Cynap -järjestelmää siis voidaan käyttää monella eri tavalla. Eri tiloissa voidaan käyttää tarpeen mukaan erilaisia konfiguraatioita.

2.8.3 Tietoverkon vaatimukset

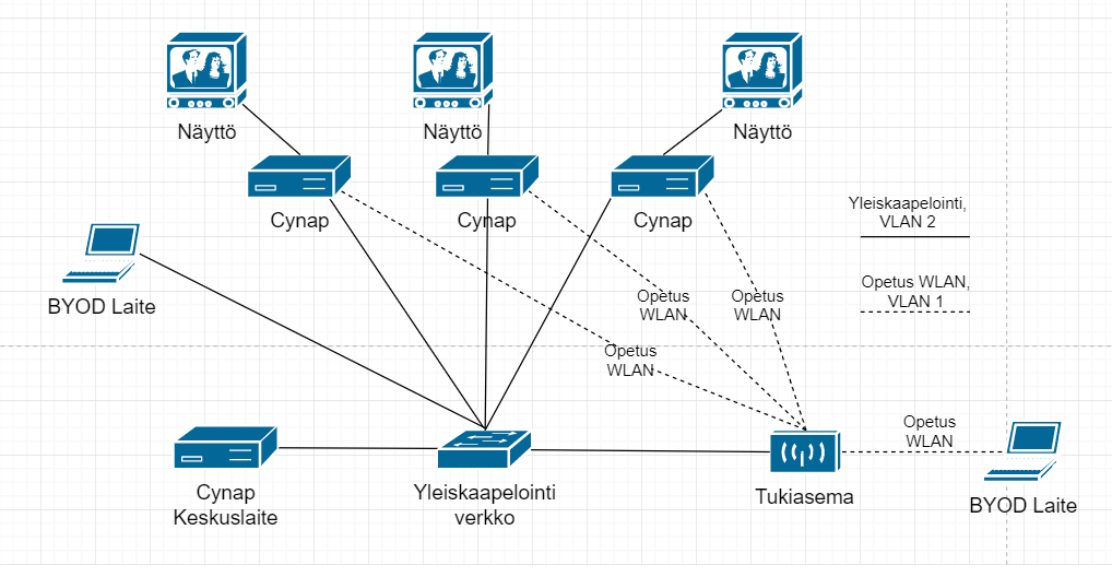
Cynap -järjestelmä perustuu paljon tietoverkon toimintaan, joten se asettaa verkolle vaatimuksia, jotta järjestelmä toimii oikein. Cynap -järjestelmä voi jakaa omaa WLAN -verkkoaan, tai se voi liittyä ulkoiseen WLAN -verkkoon. Cynapin omasta jakamasta WLANsta ei pääse koskaan internettiin. Cynap voi liittyä 2.4 Ghz:n tai 5 Ghz:n verkkoihin. Cynap -järjestelmän verkotuksessa on muutamia tekijöitä, jotka on otettava huomioon. Jos BYOD laitteet ja Cynap laite ovat eri aliverkoissa, ei laitteiden langattoman kuvansiirron protokollat, kuten Airplay ja Chromecast, tunnista Cynap Core -laitetta automaattisesti. Siksi Cynap sekä sitä käyttävät laitteet tulisi olla samassa aliverkossa, jotta automaattinen tunnistaminen toimii. Kuitenkin infrastructure -tilassa laite on näkyvillä kahdesta eri verkosta, sillä se liittyy kahteen eri verkkoon Ethernet-

sekä WLAN -rajapinnoista. Tilanne on esitelty kuviossa 13. Kuvion tapauksessa Opetus WLAN voisi olla myös samaa VLAN verkkoa ”Yleiskaapelointi VLAN” verkon kanssa. (Theiner 2018, 3-24.)



Kuvio 13. Infrastructure tilan järjestelmäkaavioesimerkki

Infrastructure -konfiguraatiota voidaan käyttää myös vSolution Matrix ratkaisussa. Matrix ratkaisussa keskuslaite ohjailee useampaa Cynap -laitetta. Keskuslaitteen sekä Cynap -laitteiden tulee silloin olla samassa verkossa, joka tässä esimerkin tapauksessa on Yleiskaapelointi VLAN 2 verkko. Kuitenkin ongelmaksi tulee silloin se, että laitteet, jotka ovat yhdistettynä langattomasti Opetus WLAN -verkkoon, eivät pysty yhdistämään laitteisiin sillä ne ovat eri verkossa. Ongelma ratkaistaan käyttämällä Cynap laitteita Infrastructure tilassa, jolloin ne yhdistetään molempiin verkkoihin, langattomaan sekä langalliseen verkkoon kuvion 14 mukaisesti. (Theiner 2018, 31-32.)



Kuvio 14 vSolution Matrix Infrastructure -konfiguraatiossa

Eli BYOD päätelaitteet ja Cynap halutaan olevan samassa verkossa, jotta laitteet löytävät Cynapin, saavat siihen yhteyden, ja voivat jakaa haluamaansa mediaa. Kuitenkin mikäli laitetta käytetään Infrastructure -tilassa, ei voida käyttää samaan aikaan Miracast Peer-to-Peer yhteyttä laitteeseen, vaan saatavilla on silloin vain tietoverkkoa hyödyntävät protokollat kuten Airplay ja Chromecast.

Cynap -järjestelmä tukee multicast -lähetystä. Multicastin avulla Cynap voi streamata usealle eri päätelaitteelle yhtäaikaisesti. Multicast -lähetyksen voi ajatella ”yksi lähetys usealle” kun taas Unicast -lähetys olisi ”monta lähetystä monelle”. Multicast siis kuormittaa verkkoa huomattavasti vähemmän. Cynap tukee RTP multicast -lähetystä LAN 1 -rajapinnasta. Kaikki muut samassa verkossa voivat halutessaan liittyä seuraamaan/kuuntelemaan lähetystä. Multicastia käytettäessä kytkimen portit on muistettava kytkeä IGMP snooping -tilaan, jolloin lähetyksellä ei turhaan tukita verkkoa lähettämällä lähetystä vastaanottajille, jotka eivät lähetystä kuuntele. Kaikki laitteet eivät välttämättä tue multicast -lähetystä, jolloin on käytettävä RSTP Unicast -lähetystä, jolloin jokaiselle lähetyksen kuuntelijalle avataan oma lähetyksensä. Cynap -

laitteella voidaan myös kuunnella muiden lähetyksiä, esimerkiksi toisen Cynap -laitteen lähettämää lähetystä tai vaikka turvakameran lähetystä. (Theiner 2018, 3-24.)

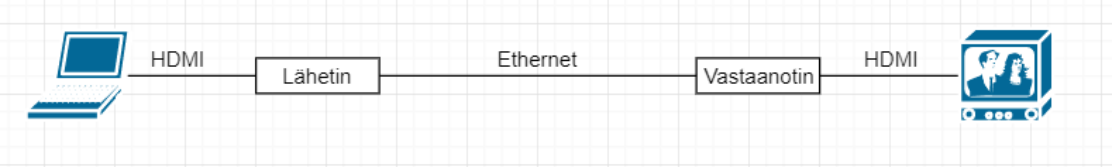
2.9 Audiovisuaaliset järjestelmät (Crestron)

2.9.1 Yleistä

Crestron tuottaa audiovisuaalisia ratkaisuita yrityksille, koulurakennuksiin, kokoushuoneisiin ja melkein mihin tahansa. Crestron tarjoaa helppokäyttöisiä työkaluja, joilla voidaan helposti esimerkiksi streamata videota, esittää dokumentti tai toistaa luennon materiaalia. Crestronin järjestelmät tukevat satoja huoneita rakennuksessa, hyödyntäen olemassa olevaa infrastruktuuria. Crestron järjestelmään voidaan ottaa myös etähallintayhteys, jolla voidaan esimerkiksi paikantaa vikoja tai hallita järjestelmää. Crestron järjestelmä tukee myös langatonta kuvansiirtoa, jolloin esimerkiksi puhelimella tai tabletilla voidaan jakaa sisältöä monitoreille langattomasti. (Education Solutions 2019.)

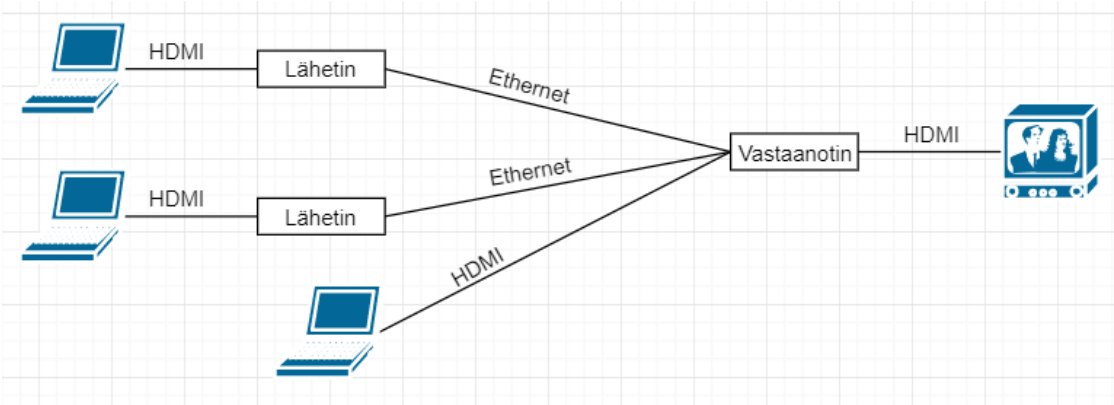
2.9.2 Toimintaperiaate

Crestron järjestelmä voidaan toteuttaa monella eri tavalla. Järjestelmä voi olla Point-to-Point konfiguraatiolla, jolloin data siirtyy kahden pisteen välillä. Tämä konfiguraatio koostuu lähettimistä, joihin tulee esimerkiksi tietokoneelta HDMI IN, sekä vastaanottimelta, josta lähtee näytölle HDMI OUT. Tämä konfiguraatio käy hyvin pienempiin tiloihin, joita ei välttämättä haluta yhdistää muiden tilojen järjestelmiin ollenkaan. Lähettimiä ja vastaanottimia käytetään kuljettamaan 4K kuvaa pidemmälle kuin pelkkä HDMI kaapeli tukisi. Yksinkertainen asetelma on kuvattuna kuviossa 15. (HD-TX-101-C-1G-E-B-T 2019.)



Kuvio 15 Yksinkertainen Point-To-Point konfiguraatio

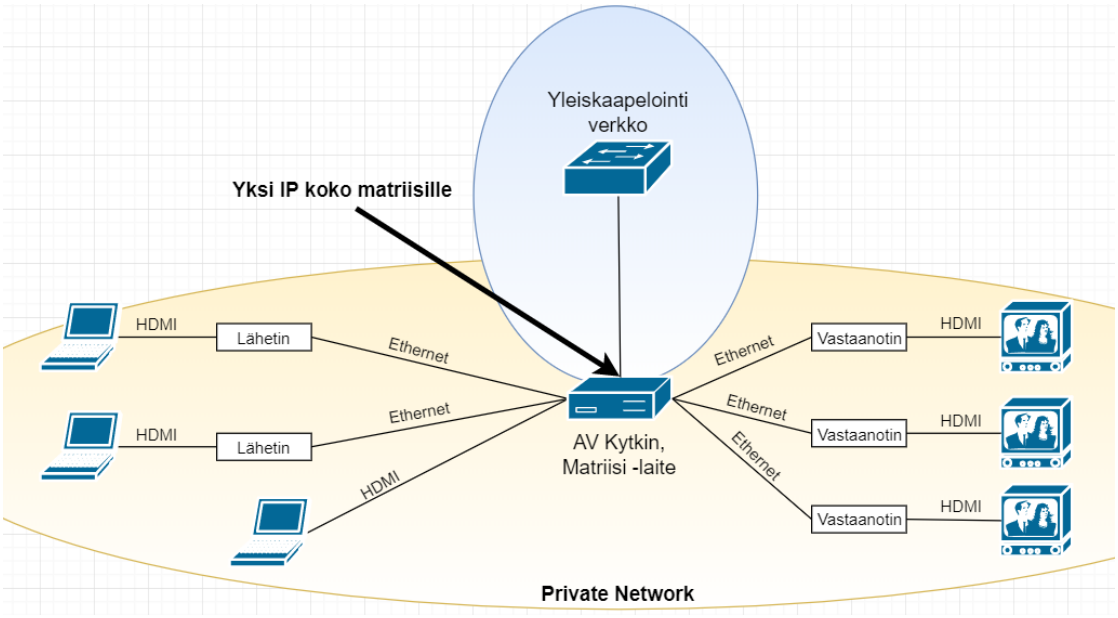
Crestron myös valmistaa vastaanottimia, joihin voi liittää myös useamman lähettimen. Vastaanottimelta lähtee sitten yksi HDMI OUT, johon voidaan syöttää kuvaa lähettimiltä. Tämä toteutus on kuvattuna kuviossa 16. (HD-RX-4K-410-C-E 2019.)



Kuvio 16 Useamman lähettimen Point-To-Point -konfiguraatio

Järjestelmän kokoa voidaan kasvattaa matriisi konfiguraatiolla, jolloin järjestelmään liitetään mukaan matriisi -laite. Matriisi -laitteeseen voidaan liittää sitten useampia lähettimiä ja vastaanottimia, jolloin kuvaa voidaan lähettää esimerkiksi yhdestä pisteestä useampaan pisteeseen sekä eri pisteisiin. Tässä konfiguraatiossa matriisi -laite siis jakaa liikennettä pisteiden välillä, sekä liikennettä voidaan hallita matriisi -laitteen kautta, liittämällä se tietoverkkoon. Näin koko järjestelmää voidaan hallita matriisi -laitteelta yhdestä pisteestä käytännössä yhdellä IP-osoitteella. AV -kytkin luo siis oman AV matriisin. Tämä matriisi on täysin erillään rakennuksen tietoverkosta, sillä laite luo oman verkon lähettimille ja vastaanottimille Private Network Mode -tekniikalla. Silloin rakennuksen tietoverkossa näkyy vain yksi laite eli matriisi -laite, josta hallitaan matriisia. Matriisi voidaan yhtä hyvin jättää kokonaan yhdistämättä tietoverkkoon. Erillään olevaa matriisia hallitaan silloin ohjain -laitteella. Tietoverkkoon

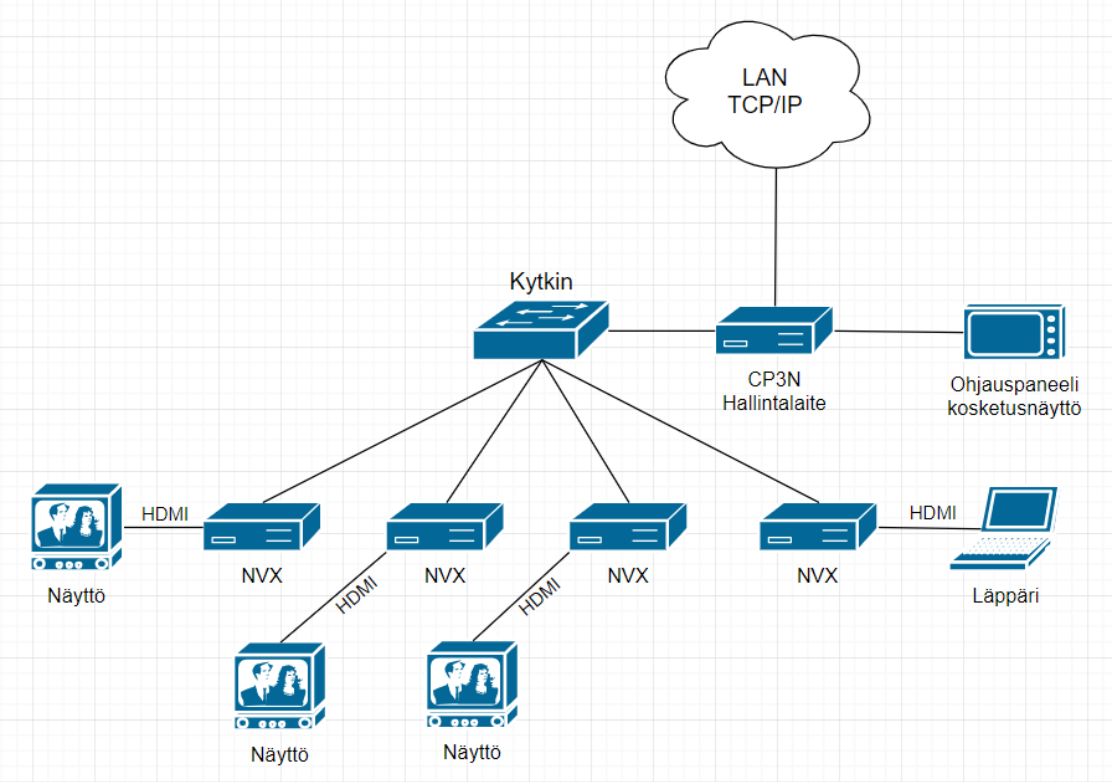
yhdistetty matriisi -asetelma on esitelty kuviossa 17. (Crestron® DigitalMedia™ System 2019, 68-69; DM-MD8X8-CPU3 2019.)



Kuvio 17 AV -kytkimellä luotu erillinen AV matriisi

Nykyään on paljon käytössä AV-over-IP -tekniikat. Tämä tarkoittaa sitä, että AV lähettimet ja vastaanottimet kytketään tietoverkkoon, jonka ylitse ne keskustelevat toisilleen ja jakavat sisältöä. Crestronilla tätä tekniikkaa kutsutaan NVX tekniikaksi. NVX tekniikkaa voi käyttää todella monella tavalla ja eri verkkotopologioilla. Järjestelmä koostuu NVX laitteista, jotka toimivat lähettiminä sekä vastaanottimina. Tämä tarkoittaa sitä, että NVX laitteisiin kytketään päätelaitteita kuten näyttöjä, joilta toistetaan sisältöä sekä tietokoneita, jotka lähettävät sisältöä NVX lähettimille. NVX laitteet yhdistetään tietoverkkoon ja virtaa yleensä syötetään niille PoE -tekniikalla (Power Over Ethernet). Pienemmissä kokonaisuuksissa voidaan käyttää esimerkiksi vain yhtä verkkokytkintä, johon liitetään kaikki tilan NVX laitteet. Tällöin kyseessä on tähti -to-

pologia. NVX verkkoon kytketään usein laite, jolla hallitaan NVX laitteita. Näillä hallintalaitteilla voidaan myös eristää AV verkko julkisesta LAN verkosta, jolloin topologia yksinkertaistuu. Topologia voisi silloin olla esimerkiksi kuvion 18 mukainen. (DM NVX Application Design Guide 2018, 7-15; DM NVX™ AV-over-IP System 2019, 16-19)



Kuvio 18 NVX eristetty tähti -topologia

Edellä mainittu esimerkki voisi olla esimerkiksi liikuntasali, jossa esitetään esimerkiksi juhlia ja näytöksiä.

2.9.3 Tietoverkon vaatimukset

NVX tekniikka pakkaa jopa 4K 60 fps videon kulkemaan 1 Gbit/s tietoverkossa, joten kytkimen porteiksi riittää 1Gbit/s portit, joihin NVX -laitteet liitetään. Jos lähetyksiä halutaan lähettää yhden kytkimen tähtitopologiasta muualle esimerkiksi toisen tähti-

topologian laitteisiin, on kytkimen Uplinkin silloin oltava tarpeeksi järeä tukemaan lähetyksiä. Esimerkiksi kytkin, jossa on 40 NVX -laitetta tarvitsisi 40 Gbit/s Uplinkin jos halutaan lähettää 40 lähetystä Uplinkkiä pitkin muualle. (Ann Earon N.d, 2-13; DM NVX Application Design Guide 2018, 2)

Multicast on olennainen osa koko systeemiä, ja NVX -tekniikka tarvitsee Layer 3 -kytkimen laitteekseen. Jopa kahden NVX laitteen välinen tiedonsiirto tapahtuu multicast lähetyksellä, joten se on pakollinen ominaisuus. Kytkimellä on hyvä luoda oma VLAN kaikille NVX -laitteille. Jotta multicast lähetystä voidaan lähettää vain niille osallistujille, jotka sitä haluavat, on kytkimen porteissa oltava IGMP snooping konfiguroituna. NVX tukee sekä IGMPv2 että IGMPv3 protokollia. Kytkin tulee myös konfiguroida käyttäytymään IGMP Querier -tilassa. Multicast lähetyksissä suositellaan käytettävän isossa NVX verkossa PIM-SM (Protocol Independent Multicast, Sparse-Mode) lähetystä, sillä se skaalautuu parhaiten. (DM NVX™ AV-over-IP System 2019, 21-23).

Mikäli halutaan eristää NVX verkko kokonaan ”julkisesta” LAN verkosta, CP3N tai muu kontrolleri, joka voi luoda Control Subnetin on hyvä valinta. Tällöin CP3N toimii DHCP sekä DNS serverinä, ja jakaa näin automaattisesti NVX laitteille osoitteet, sekä löytää ne. Tämä verkko jää täysin erilliseksi julkisesta verkosta, jolloin NVX laitteet eivät näy sinne, eikä niitä voida hallita lainkaan LAN verkosta. Hallinnointi tapahtuu silloin kontrollerin kautta, esimerkiksi Touchpadin avulla tai ottamalla tietoverkon kautta yhteys CP3N -hallintalaitteeseen, josta järjestelmää voidaan hallita myös etänä. Etuna tässä on se, että esimerkiksi Multicast lähetykset eivät vahingossakaan tuki julkista verkkoa, sekä NVX laitteilla on täysin eristetty oma verkkonsa, jota eivät häiritse muut laitteet. Haittana on se, että NVX laitteita ei nähdä julkisesta verkosta, vaan kaikki hallinnointi tapahtuu kontrollerin kautta. Julkisesta LAN verkosta nähdään kuitenkin kontrollerilaite. Huomion arvoista on myös se, että tästä Control Subnetistä ei ole pääsyä internettiin. (3-Series® Control Systems 2019, 33-36).

2.10 Tietoturvallisuus

Tietoverkon olennainen osa on luoda siitä tietoturvallinen. Tietoverkossa voi kulkea arkaluontoista dataa, joka halutaan pitää tallessa ja suojata se väärinkäytöltä. Tietoturvallisuus on laaja käsite, joka sisältää useita pienempiä osa-alueita, joista tässä avataan muutamia. Ensimmäinen osa-alue on pääsyoikeudet ja listat. Nämä määrittävät sen kenellä on pääsy mihinkin osaan verkkoa. Listoissa ei haluta sallia sellaisia pääsyoikeuksia, joita ei tarvita. Seuraavana tietoturvallisuuden osa-alueena on haittaohjelmilta suojautuminen. Tämä toteutetaan yleensä virustorjuntaohjelmilla, jotka tunnistavat mahdolliset haittaohjelmat ja poistavat ne.

Tietoturvaan kuuluu olennaisesti järjestelmät ja niiden turvallisuus. Ovatko käytössä olevat järjestelmät testattuja ja turvallisia? Monissa järjestelmissä on aukkoja, joita hyökkääjät voivat hyödyntää. Tämä estetään parhaiten valitsemalla käytettäväksi sellaiset järjestelmät, joita päivitetään sekä niitä testataan tietoturvan kannalta.

Monitoroinnilla ja tietoverkon analysoinnilla parannetaan tietoturvallisuutta. Silloin kun tiedetään, minkälainen verkon käyttäytyminen on normaalia, huomataan jos siellä tapahtuu jotain epänormaalia. Silloin epänormaalit voidaan tarkistaa ja estää, jos kyseessä on jotain epämääräistä toimintaa.

Tietojen häviämisen estäminen tehdään usein varmuuskopioimalla sellaista dataa, jonka ei haluta poistuvan. Aina on muistettava, että mikä tahansa yksittäinen laite voi hajota, jolloin sen sisältämät tiedot voivat olla vaarassa, jos varmuuskopiointeja ei ole tehty.

Palomuurit sekä sähköpostiliikenteen suodattimet ja filtterit ovat olennainen osa tietoturvallisuutta. Palomuureilla luodaan raja luotetun verkon sekä epäluotettavan verkon välille, eli Internetin. Palomuurit sisältävät usein sääntöjä, jolla liikennettä joko sallitaan tai estetään. Sähköpostisuodattimet taas filtteröivät sähköpostiliikenteestä spam -viestejä, epäluotettuja lähettäjiä sekä haittaohjelmia tai linkkejä. (What Is Network Security N.d.).

2.11 Ylläpito

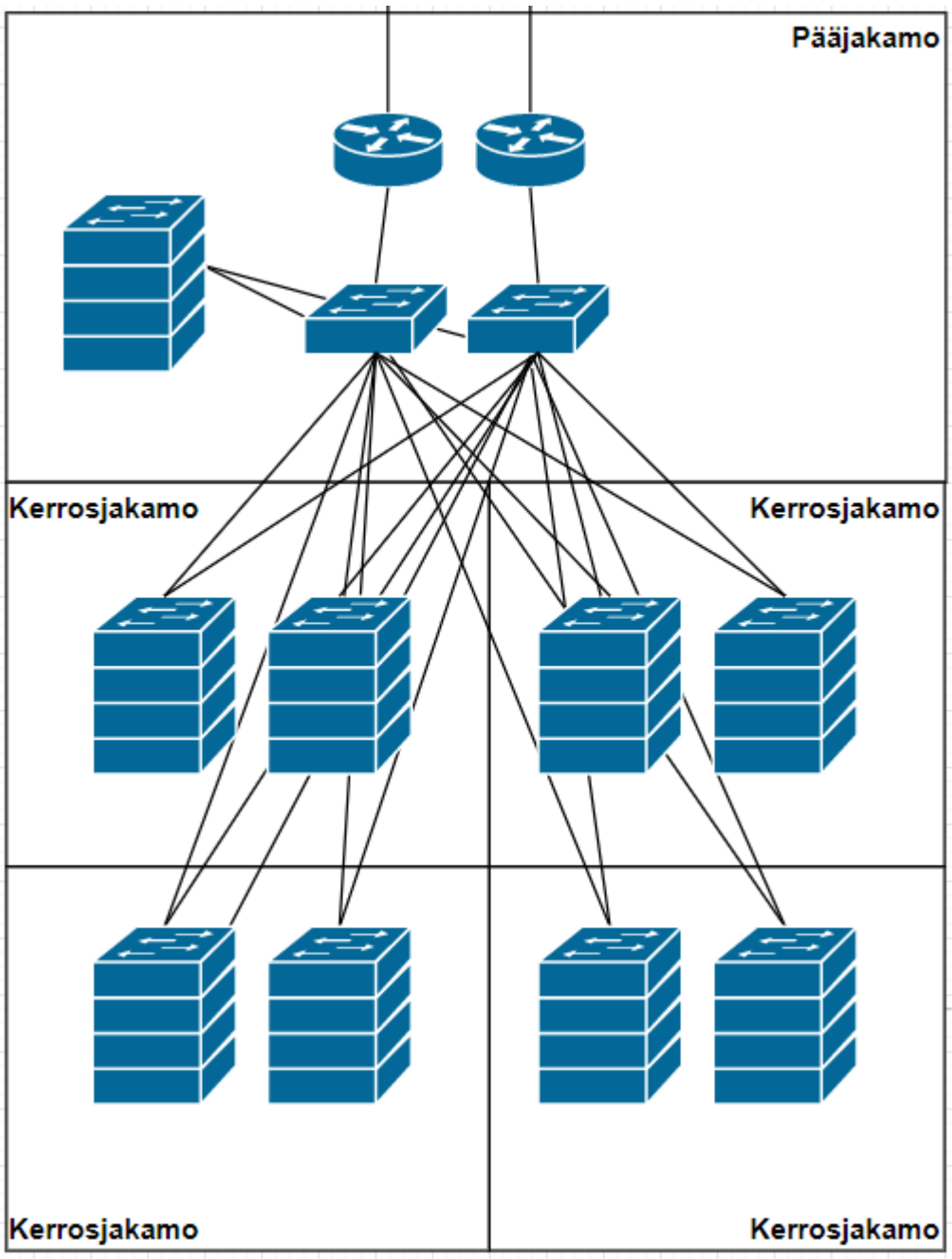
Tietoverkon ylläpitoon kuuluu muutamia aihealueita. Vikatilanteita halutaan välttää tietoverkossa, joten viat halutaan tunnistaa ja huomata mahdollisimman aikaisin. Laitteet voivat olla konfiguroitu hälyttämään tai välittämään ilmoituksen, jos ne huomaavat kriittisen linjan vikaantumisen. Seuraavaksi vika halutaan rajata ja tunnistaa mahdollisimman tarkasti. Kun vika on selvillä, voidaan toteuttaa korjaustoimenpiteet. Nopea vianhallinta on osa tietoverkon ylläpitoa. Toisena on laitteiden konfiguraatioiden, lisenssien sekä ohjelmistoversioiden ylläpito. Konfiguraatiot laitteilta tulee säilyttää hyvässä tallessa, sekä säilyttää myös aiemmat versiot konfiguraatiosta. Tietoverkon ylläpitäjän tulee myös huolehtia laitteiden lisensseistä ja ohjelmistopäivityksistä, että ne ovat ajan tasalla. Ylläpitoon kuuluu olennaisena tietoverkon monitorointi. Monitoroinnilla ennaltaehkäistään vikatilanteita ja ongelmakohtiin voidaan puuttua, ennen kuin loppukäyttäjä huomaa ongelmaa. Monitoroinnilla tarkastellaan laitteiden suorituskykyä ja verkossa kulkevaa liikenteen määrää. Myös lokien monitorointi ja suodattaminen on tärkeää. Ylläpitoon kuuluu olennaisesti myös tietoturvallisuuden ylläpito. Esimerkiksi järjestelmistä poistetaan käyttäjät, joita ei enää tarvita sekä annetaan pääsyoikeuksia vain varmistetuille käyttäjille. Lisäksi halutaan aina olla selvillä, kuka tai keillä on oikeudet järjestelmiin. (Network Management System 2018.)

3 Aiempien ratkaisuiden tarkastelu

3.1 Fyysinen verkon rakenne

Yleensä tietoverkon aktiivilaitteiden hankinta sekä ylläpito on tilaajan vastuulla. Tästä syystä ei voida tarkasti tietää millainen verkkojen rakenne todellisuudessa on, mutta voidaan hahmotella sen pääpiirteitä kaapelointien perusteella. Fyysisen tietoverkon

rakenne koostuu lähes aina pääjakamosta sekä kerrosjakamoista. Pääjakamoon tulevat reitittimet, joista on liitynnät operaattoreihin eli ulkoverkkoon. Pääjakamon pääkaapissa on myös paneelit nousukaapeloinnille, eli niille kaapeleille, joilla yhdistetään kerrosjakamot pääjakamoon. Voidaan olettaa, että pääkaappiin tulee kuitukytkimet, josta lähtevät nousukaapeloinnit kerrosjakamoihin, sekä reitittimiin menevät kaapelit. Kerrosjakamot koostuvat laitekaapeista, joihin tulee kytkimiä. Kytkimistä lähtevät kaapeloinnit RJ45 liittimillä oleviin seinärasioihin, joihin loppukäyttäjä voi liittää päätelaitteensa, tai joihin liitetään muita laitteita esimerkiksi valvontakameroita. Kerrosjakamot liitetään pääjakamoon kuitukaapelein sekä joskus varalta myös kuparikaapelein. Jos pääkaapissa on kuitukytkimet erikseen kerrosjakamoiden yhdistämiseen, on fyysinen verkkomalli silloin hierarkkinen, eli kolmitasoinen. Kuvioon 19 on hahmoteltu sellaisen verkon mallia, mikä on rakennettu tällä perinteisellä kaavalla. Kuvio on vain suuntaa antava, ja todelliset verkkokuvat saattavat erota hahmotellusta kuviosta.



Kuvio 19. Fyysinen hahmoteltu verkkokuva

3.2 Kaapeloinnit

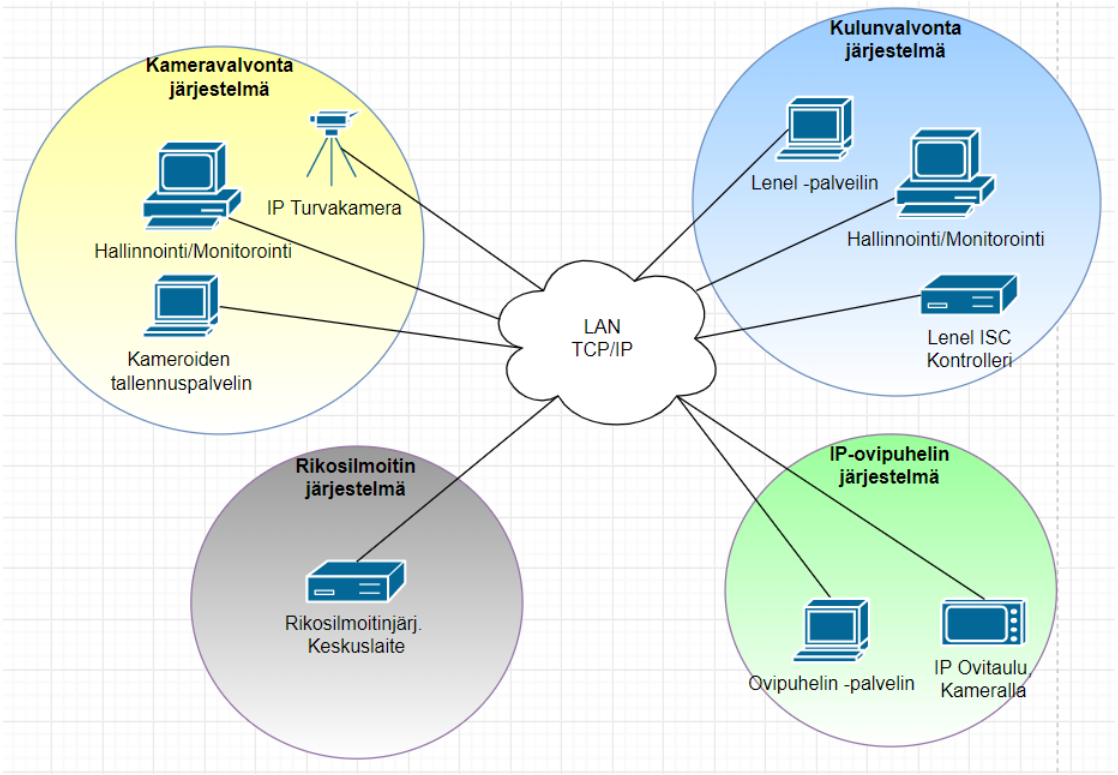
Usein kouluissa käytetään kuitu- sekä kuparikaapeleita. Kuparikaapelit ovat usein nykyään luokkaa CAT6a, eli jokaisella kuparikaapelilla on teoreettinen siirtokapasiteetti

10Gbit/s aina 100m asti. Suojauksina kuparikaapeleissa käytetään U/FTP suojausta, tarkoittaen että kaikki kaapelissa olevat kupariparit ovat foliosuojattuja, mikä poistaa kaapeleista niihin aiheutuvia sähkömagneettisia häiriöitä.

Kuitukaapeleiksi on valittu usein käytettäväksi OS2 yksimuotokuitua, sekä OM3 -luokan monimuotokaapelia. Ulkotiloihin tulee ainoistaan yksimuotokaapelia. Varmentaviin yhteyksiin on valittu yksimuotoa, sekä OM3 monimuotokaapelia. Kaapeleita kulkee siis reilu määrä verkossa, eli vikatilanteessa voidaan esimerkiksi vain kytkeä toinen kuitulinja käyttöön. Myös kaistanlisäys onnistuu näin kytkemällä toisia kuituja käyttöön.

3.3 Tietoverkkoon liittyvät järjestelmät

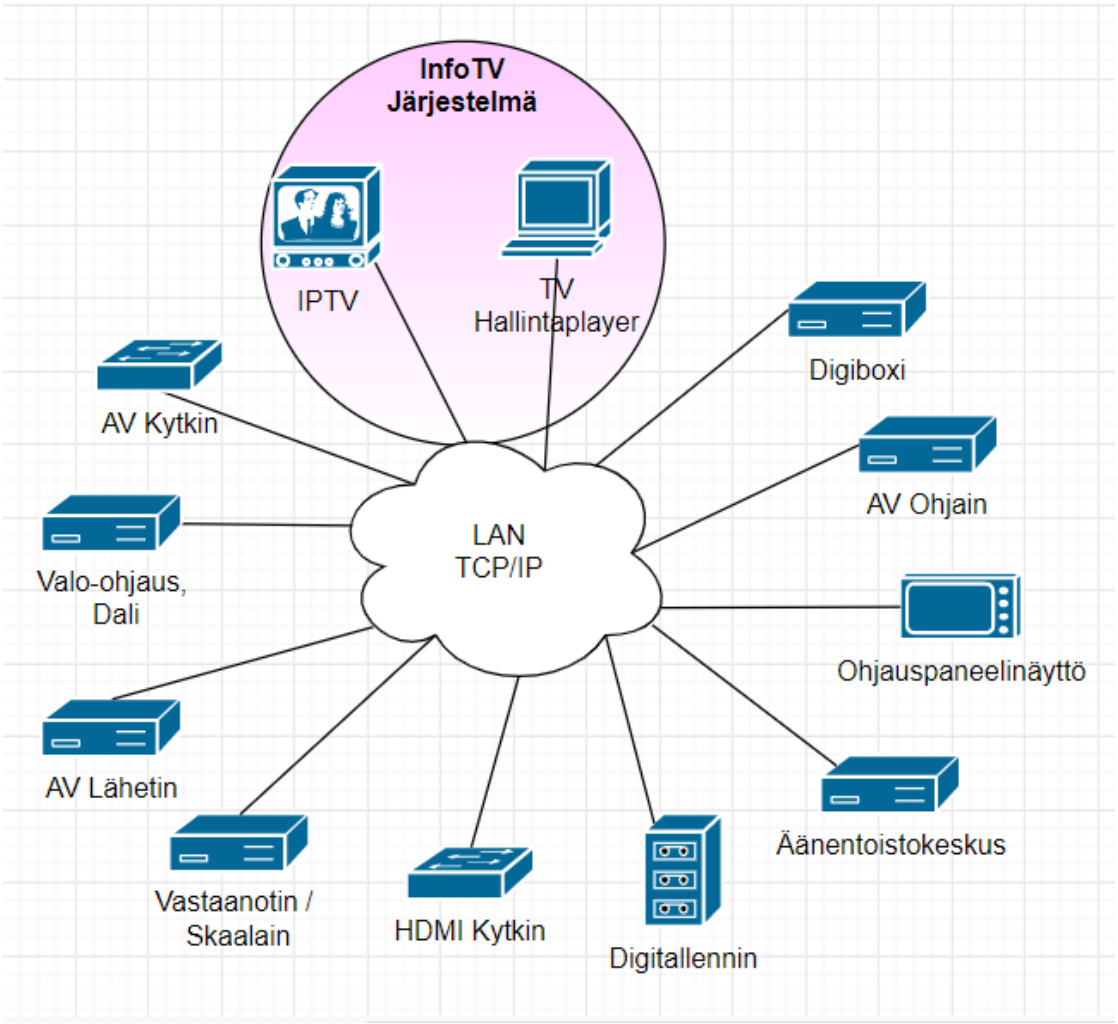
Tietoverkkoon liitettävät järjestelmät riippuvat siitä, mitä tilaaja haluaa. Nykyään rakennettaviin kouluihin tulee usein Lenel -järjestelmä, tai jokin muu kulunhallintajärjestelmä, jolla ohjataan monia toimintoja sekä se keskustelee useiden eri järjestelmien kanssa. Lenel -järjestelmä toimii mm. Kulunvalvontajärjestelmän pääohjaimena, langattomien Aperio lukkojen hubien ohjaimena, rikosilmoitinjärjestelmän ohjaimena ja IP-pohjaisen ovipuhelinjärjestelmän kanssa. Lenel on siis tärkeässä roolissa turvajärjestelmien hallinnassa. Lenel palvelinohjelmisto voidaan asentaa fyysiselle palvelimelle, joka sijaitsee rakennuksessa tai vastaavasti virtualisoida se esimerkiksi konesaliin. IP rajapinta näille järjestelmille on kulunvalvonnan kaappi, jossa on järjestelmien tarvitsemat kontrollerit/keskuslaitteet. Kontrollerit ja keskuslaitteet em. järjestelmille kytkeytyvät siis IP-verkkoon, jolloin ne otetaan huomioon verkkosuunnittelussa. Tietoverkon yli keskustelevia laitteita on kuvattuna kuviossa 20.



Kuvio 20. Tietoverkkoon kytkettäviä järjestelmiä

3.4 Tietoverkkoon liittyvät audiovisuaaliset laitteet

Verkkoon usein myös liitetään paljon audiovisuaalisia laitteita, kuten infonäyttöjä, tai luokkien AV-vastaanottimia. Näillä laitteilla saattaa olla tietoverkolle erilaisia vaatimuksia kuin esimerkiksi normaalilla työasemalla, siksi ne on hyvä kuvata erikseen. Tiloissa, joissa on paljon AV laitteita, jotka yhdistyvät verkkoon, löytyvät usein omat AV kytkimet. AV kytkimiin liitetään tilan AV järjestelmät, ja kytkin sitten liitetään kerrosjakamon kytkimeen. AV Laitteistoa, jota on yleensä liitetty tietoverkkoon, esitellään kuviossa 21.



Kuvio 21. Tietoverkkoon liitettävää AV -laitteistoa

3.5 Esiintyneitä ongelmia

Vastaan on tullut muutamia ongelmia. Ensimmäinen ongelma on ollut Caverionin etäyhteyspalvelin, eli Tosibox -palvelin. Tosibox on palvelin, joka muodostaa VPN yhteyden työasemaan, johon kytketään Tosibox avain. Tällöin työasema pääsee etänä samaan verkkoon kuin missä Tosibox fyysisesti on kytkettynä. Tosibox on todella yksinkertainen käyttää etäyhteyspalvelimena, mutta se on aiheuttanut joitakin ongelmia verkossa, kuten että kytkimen portti missä sellainen on ollut kiinni, on pumpannut, eli portti on sulkeutunut ja avautunut toistuvasti.

Toinen esiintynyt ongelma on ollut Aperion langattomien lukkojen kaistapäällekkäisyydet, ja niistä aiheutuneet signaalihäiriöt. Aperio -lukot keskustelevat Hubin kanssa Hubin jakaman 2.4 Ghz verkon ylitse, kanavilla 11-26. Häiriöitä on esiintynyt, sillä kanavat ovat menneet päällekkäin rakennuksen oman 2.4 Ghz langattoman Wifi verkon kanssa.

Ongelmaksi on myös joissain tapauksissa koettu tietoturvallisuus. Tällä hetkellä järjestelmiä on kytkettynä tilaajien verkossa, jossa se on ulkoinen tekijä. Nämä haluttaisiin erottaa kokonaan ja erottamiseen haluttaisiin ratkaisu. Ratkaisuksi on ehdotettu esimerkiksi Caverionin järjestelmille rakennettavaksi kokonaan omaa fyysistä verkkoa ja tilaajalle omaa fyysistä verkkoa. Kaksi fyysistä verkkoa ja ulkoverkkoliittymää on tietysti kaikista varmin ratkaisu, mutta ei varmasti kustannustehokkain.

AV Järjestelmissä on muutamia asioita, jotka on koettu ongelmaksi koskien tietoverkkoa. Langattomassa kuvansiirrossa haasteita on ollut siinä, että jos vastaanottava ja lähettävä laite ovat eri verkoissa, ne eivät voi jutella keskenään ja kuvansiirto ei onnistu. Tämä on voitu korjata esimerkiksi vaihtamalla langatonta verkkoa siihen verkkoon, missä langattoman kuvansiirron vastaanottava laite on, mutta verkkojen edestakainen hyppiminen tietysti hidastaa asioita. Eli halutaan ratkaisu siihen, että esimerkiksi Guest- sekä Opetusverkoista voitaisi molemmista käyttää laitetta. Myös se, että jos yhdistää langattoman vastaanottimen jakamaan verkkoon, laitteella ei ole enää pääsyä internettiin on hankaloittanut esimerkiksi sisällön jakoa. NVX Tekniikassa haasteita on tuottanut myös kytkinlaite. NVX on ollut haasteellinen toteuttaa tietyillä kytkimillä, joten kytkinlaitetta hankkiessa tulee olla tarkka sen vaatimuksista.

Ei niinkään ongelma, mutta parannusehdotus on tullut ilmi koskien palvelimia. Eli esimerkiksi kulunvalvonnan palvelimet, ja muut palvelimet haluttaisiin fyysisesti siirtää muualle rakennuksista, minkä voisi korjata virtualisoimalla palvelimia esimerkiksi konesaleihin.

4 Tavoitetilan määrittely

Kuten aiemmassa JHS179 -kappaleessa todettiin, on suunnittelussa hyvä lähteä liikkeelle siitä, mikä on nykytila. Nykytilana voimme käyttää esimerkiksi tuoreinta koulun verkkoa ja sen järjestelmiä. Nykytilasta pyritään löytämään ongelmakohtia ja sellaisia kohtia tai ominaisuuksia, joita haluamme muuttaa. Seuraavaksi lähdetään määrittämään tavoitetilaa. Tavoitetila on tila, johon pyritään koko suunnittelu- sekä toteutusprosessin ajan. Kun tavoitetila on selvillä, voimme mitoittaa ja suunnitella tietoverkon rakennukseen. Tavoitetilan kartoituksessa mietitään, mitä verkolta oikeasti halutaan ja tarvitaan. Tavoitteessa on otettava huomioon myös mahdollinen laajentumisvara tulevaisuutta ajatellen. Tavoitetilaa suunniteltaessa voimme jakaa erilaisia osa-alueita pienempiin palasiin, ja koota ne lopuksi yhdeksi tavoitetilaksi. Jokaiselle verkon osa-alueelle mietitään mahdollisimman tarkasti sen tarvitsemat ominaisuudet.

4.1 Käyttäjämäärä

Tietoverkossa otetaan ensisijaisesti huomioon sen käyttäjät, eli koulurakennuksen tapauksessa oppilaat sekä opettajat, joille tarjotaan Internet -yhteys. Tietoverkon kapasiteettisuunnittelussa täytyy tietää suunnilleen, montako oppilasta ja työntekijää kouluun tulee.

Käyttäjän tarvitsema kapasiteetti riippuu siitä, mihin yhteyttä käytetään. Esimerkiksi videoiden tai suoratoiston katselu tarvitsee enemmän kaistaa, kuin täysin normaali internet selailu. Kuitenkin videoiden katselu, videopuheluiden soittaminen ja muut enemmän kapasiteettia tarvitsevat tekniikat yleistyvät. Yhden käyttäjän käyttämää tarkkaa kapasiteettia on vaikea tietää tarkasti. Käyttäjän tarvitsema kapasiteetti saattaa myös muuttua monessa tilanteessa. Kuitenkin arvio yhden käyttäjän tarvitsemasta kaistanleveydestä internet -liitynnältä, eli ISP -yhteydeltä on 4.3 Mbit/s, vuosina 2020-2021 opetusympäristöissä. Vuosille 2017-2018 arvio on ollut 1.5Mbit/s per

käyttäjä. (Fox, Jones 2016, 2.) Käyttäjien tarvitsema kokonaiskaistan leveys voidaan siis arvioida laskemalla käyttäjämäärä kerrottuna kulutusarviolla, jos kaikki käyttäisivät yhteyttä samaan aikaan. Mitoituksessa voidaan ajatella, montako oppilasta koulussa tulee olemaan samanaikaisesti. Voi olla esimerkiksi tilanne, jossa koulussa opiskelee 500 oppilasta, mutta siellä ei koskaan ole samanaikaisesti yli 400 henkeä, silloin laskelma voidaan tehdä käyttämällä 400 henkilön lukua. Täytyy myös ottaa huomioon poikkeustilanteet, esimerkiksi juhlat, jolloin paikalla saattaa olla enemmän henkilöitä kerrallaan.

4.2 Palvelut ja järjestelmät

Seuraavaksi mietitään, mitä palveluita tavoitetilan tietoverkko tarjoaa. Palveluita voisi olla esimerkiksi langattoman verkon tarjoaminen, info-TV järjestelmä, rakennuksen langaton lukitusjärjestelmä, jne. Kartoitetaan siis mitä järjestelmiä ja palveluita rakennukseen tulee ja mitkä niiden vaatimukset ovat. Jokaisesta palvelusta, joka liittyy rakennuksen tietoverkkoon, tulee täyttää oheinen taulukko 5. Taulukkoon mietitään mitä komponentteja järjestelmään kuuluu, ja minkälaisia vaatimuksia niillä on verkolle. Taulukon 5 tiedoilla saamme hyvän yleiskuvan järjestelmästä, sen komponenteista sekä siitä mitä ne tarvitsevat tietoverkolta. Kuitenkin jokainen palvelu sekä järjestelmä tarvitsee myös syvällisen ymmärryksen toiminnastaan, jotta se voidaan tarjota käyttäjälle täysin toimivana sekä vikasietoisena. Kuitenkin taulukon tiedot järjestelmistä auttavat tietoverkon suunnittelijaa ottamaan suunnittelussa huomioon myös kaikki kiinteistötekniset järjestelmät.

Taulukko 5. Järjestelmän/Palvelun vaatimukset

Järjestelmän nimi	Komponentti 1	Komponentti 2	Komponentti 3
Määrä			
Tehtävä			

Internet, Kyllä/Ei			
DHCP/Staattinen osoite			
DNS record			
NAT			
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)			
Viive kriittisyys			
Kuorma verkolle (Per laite, arvio)			
Liityntätekniikka, RJ45/WLAN			
Tuetut kanavat (Jos WLAN)			

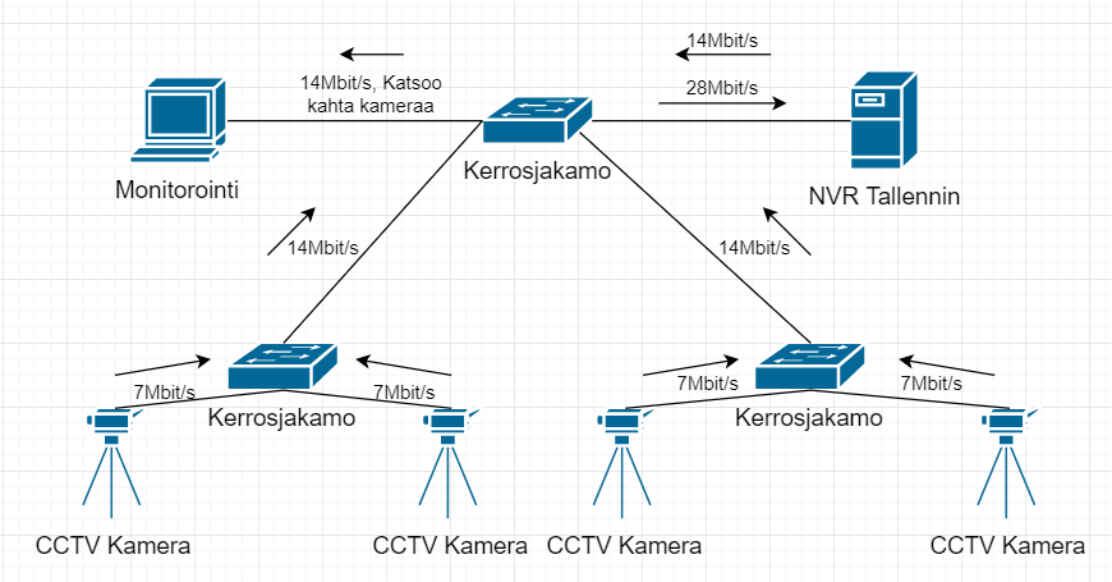
4.3 Saatavuus

Seuraavaksi tulee suunnitella ja kartoittaa, kuinka tärkeä tietoverkko ja sen palvelut ovat määrittelemällä saatavuus palveluille sekä järjestelmille. Voidaan ajatella, että esimerkiksi yksittäinen käyttäjän työasema tulisi toimia langattomassa verkossa 98% ajasta, mutta esimerkiksi kiinteistön langattomien lukkojen tulisi toimia 99.9% ajasta. Priorisoidaan siis tärkeät palvelut, jolloin ne pyritään ottamaan verkkosuunnittelussa huomioon vähentämällä kahdentamattomat solmukohdat järjestelmältä. Koulura-

kennuksissa tulee myös huomioida, että esimerkiksi tietoverkon huoltoa tai päivitystä voidaan tehdä silloin, kun koulu on suljettu. Aiemmin kartoitetuista järjestelmistä tehdään siis saatavuuden määrittely.

4.4 Kapasiteetin arviointi

Tietoverkon tehtävä on kuljettaa käyttäjien, palvelimien sekä tietoverkon komponenttien välinen liikenne. On siis arvioitava, kuinka paljon liikennettä verkossa tulee kulkemaan, jotta tietoverkon kapasiteetti voidaan mitoittaa oikein. Ylimitoitus on kallista, mutta kaikkein varmin keino. Alimitoitus taas saattaa johtaa vikatilanteisiin. Lasketaan siis aiemman järjestelmäkartoituksen sekä käyttäjälaskemien perusteella jokaisen komponentin arvioitu kuorma. Esimerkiksi 30 turvakameraa, joista jokainen lähettää dataa NVR -tallentimelle noin 7 Mbit/s, jolloin niiden yhteenlaskettu liikenne on tietoverkossa noin 210 Mbit/s. Tässä esimerkkitapauksessa tulee myös huomioida se, että mikäli NVR -tallennin on sisäverkossa kapasiteettia ei tarvitse huomioida operaattoriliitynnässä (WAN). Mikäli NVR -tallennin sijaitsee ulkoverkossa tai rakennuksen ulkopuolella, johon liikenne kulkee operaattoriliitynnän kautta, on kapasiteetti silloin huomioitava myös WAN linkissä. Kapasiteettilaskennassa on myös hyvä ajatella tulevaisuutta ja laajenemisen mahdollisuutta. Kuviossa 22 on tehty esimerkkinä kapasiteettihahmottelua neljän kameran kameravalvontajärjestelmästä, jossa NVR -tallennin on sisäverkossa. Liikennearvioita eri järjestelmille voidaan miettiä taulukon 5 perusteella. Liikennearvioita voidaan ajatella fyysisellä tasolla silloin, kun tiedetään tarkasti missä kukin komponentti sijaitsee. Jos ei vielä ole tiedossa missä laitteet fyysisesti tulevat sijaitsemaan, voidaan arvioita tehdä vain loogisella tasolla.



Kuvio 22. Kapasiteetin arvioiminen

Kun on arvioitu kaikkien järjestelmien käyttämää kaistanleveyttä, tiedetään suunnilleen mikä kohta tietoverkossa on kaikista ruuhkaisin. Tietoverkossa olevia yleiskäyttöön tarkoitettuja internet -pisteitä oppilaita ja opettajia varten sekä langatonta verkkoa voidaan ajatella erillisinä järjestelminä, jotka lasketaan mukaan. Lopputuloksena voidaan arvioida tietoverkossa kulkevaa kokonaisliikennettä ja osataan mitoittaa operaattoriliityntöihin tarpeeksi kaistanleveyttä, jotta saavutetaan tavoitetila.

WAN kaistanleveys on kalliimpaa kuin LAN kaistanleveys. Kuitenkin WAN kaistanleveyttä on oltava tarpeeksi, jotta palvelut ja järjestelmät toimivat halutulla tavalla. 80 % Kaistasta jatkuvassa käytössä oleva WAN linkki on liian ahdas. Jopa 60 % käytöllä oleva linkki on liian ahdas, sillä se saattaa huiputtaa 95 % käytöllä monia kertoja päivän aikana, jolloin se vaikuttaa negatiivisesti verkon käytettävyyteen. (How Cisco IT Uses NetFlow to Improve Network Capacity Planning, n.d.)

4.5 Kaapelointi

Tavoitetilan kaapelointi on valittava siten, että kaapelit tukevat riittävästi tiedonsiirtoa kuljettamaan kapasiteettiarvioinnin kuormaa. Mikäli tietoverkko on tavoitetilassa vikasietoinen ja halutaan esimerkiksi kahdentaa reittejä, on kaapeloinnit suunniteltava sen mukaisesti.

4.6 Verkkomallin valinta

Verkkomallin valinnassa ajatellaan tietoverkon kokoa. Tähän vaikuttaa ensisijaisesti se, kuinka paljon henkilöitä rakennuksessa tulee olemaan ja minkälaisia järjestelmiä rakennukseen tulee. Kuitenkin esimerkiksi kouluissa, yleisin verkkomalli on kolmitasoinen, joka koostuu kerrosjakamoista eli jakelukerroksesta, kuljetuskerroksesta, joka kerää kerrosjakamon laitteet yhteen sekä ydinkerroksesta eli reitittimistä, joiden kautta liitytään operaattoriin.

4.7 Internet, Etähallinta ja monitorointi

Tavoitetilaa suunniteltaessa on mietittävä, mitä kautta liikenne kulkee internettiin. Koulun tietoverkossa voi esimerkiksi olla oma internet yhteytensä, tai se voi kulkea esimerkiksi kaupungin MPLS -verkon kautta kaupungin omaan internet nieluun, jolloin koululla ei käytännössä ole paikallista internettiä, vaan liikenne internettiin kulkee muuta kautta. Valinta vaikuttaa oleellisesti tietoturvan suunnitteluun ja palomuuraukseen, etähallintaan sekä monitorointiin.

On myös mietittävä, mitkä laitteistot tai järjestelmät tarvitsevat etähallintaa. Etähallittavat laitteet sekä järjestelmät on kartoitettava, jotta tiedetään mihin kaikkiin järjestelmiin ja laitteisiin tavoitetilassa on etähallinta.

Tavoitetilassa tietoverkkoa halutaan monitoroida. Halutaan nähdä, kuinka paljon esimerkiksi dataa verkossa kulkee sekä halutaan tietää, jos jokin laite hajoaa tai järjes-

telmä kaatuu. Tavoitetilan suunnittelussa mietitään siis mitkä kaikki verkon komponentit tai järjestelmät tulevat olla monitoroinnissa, jotta vikatilanteita voidaan ennaltaehkäistä sekä reagoida niihin nopeammin.

4.8 Tietoturva

Tavoitetilan määrityksessä oleellinen osa on tietoturvallisuus. Tietoturvallisuuteen on pyrittävä fyysisellä tasolla, sekä järjestelmätasolla. Tietoturvallisen verkon suunnittelussa voidaan esimerkiksi käyttää mallia, jossa liikenne kaikkialta kielletään kaikkialle, ja sallitaan liikenne paikkoihin, johon on tarve. Toinen tapa on sallia kaikki liikenne, ja kieltää se sinne mihin liikennettä ei haluta kulkevan. Ensimmäinen tapa on tietoturvallisin. Tietoturvallisuutta voi olla haastava määrittää etukäteen, mutta voidaan ajatella, että halutaan tavoitetilan verkosta tietoturvallinen, jolloin tietoturvallisuuteen pyritään jokaisella verkon osa-alueella, suunnittelun, käyttöönoton, sekä ylläpidon ajan.

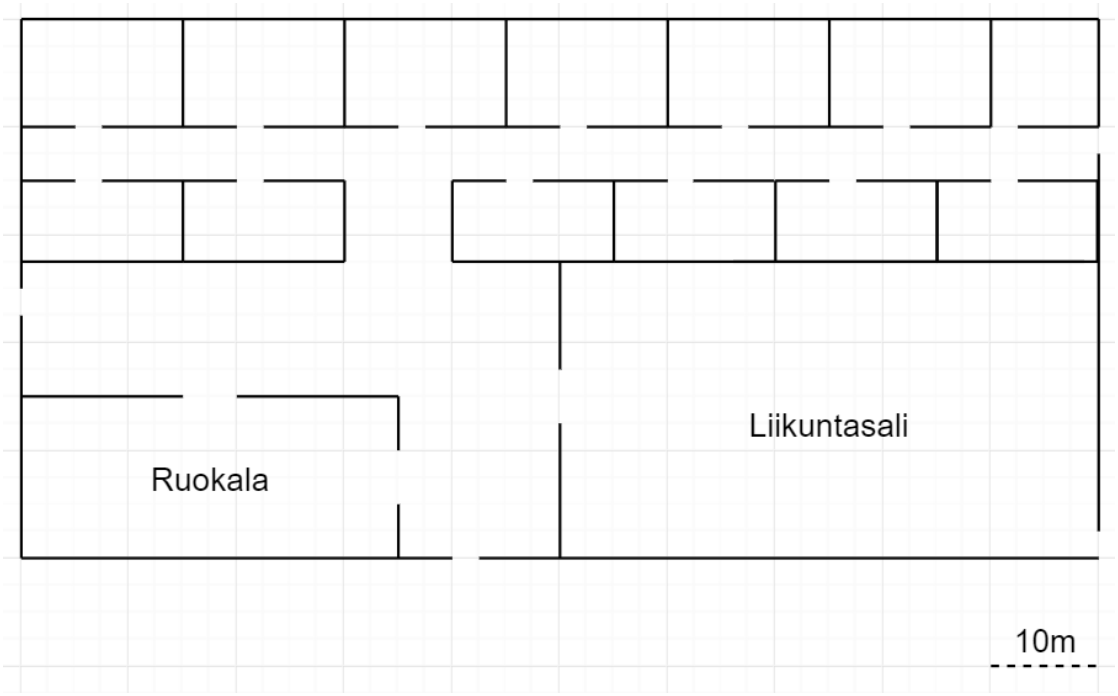
5 Esimerkki tavoitetila

5.1 Käyttäjämäärä

Kouluun tulee 300 oppilasta ja 30 opettajaa, eli yhteensä 330 henkilöä. Langattoman verkon on oltava riittävä tukemaan kaikkia käyttäjiä. Langaton verkko ajatellaan omana järjestelmänään, joten siitä on täytetty myös vaatimuskortti liitteessä 7. Langallisia RJ45 pistokkeita oppilaita sekä opettajia varten tulee olla 100 kappaletta koulussa. Kiinteää verkkoa voidaan myös ajatella omana järjestelmänään, joten se on kuvattuna liitteessä 6.

5.2 Rakennus

Pohjakuva rakennuksesta ja luokista on hahmoteltuna kuviossa 23, jonka perusteella voidaan myöhemmin tehdä langattoman verkon kanavasuunnittelu.



Kuvio 23 Kuvitteellisen koulurakennuksen pohjakuva

5.3 Palvelut ja järjestelmät

Kouluun tulevista järjestelmistä täytetään taulukon 5 mukaiset järjestelmävaatimuskortit. Kouluun tulee Lenel -kulunhallintajärjestelmä, johon sisältyy langattomat lukot ulko-oviin sekä luokkien oviin (Liite 1.), sekä kameravalvontajärjestelmä, johon kuuluu 15 kameraa (Liite 2.). Lenel palvelin virtualisoidaan konesaliin, mutta kameratallennin on koulussa. Kameravalvontajärjestelmää voidaan monitoroida yhdeltä paikalliselta työasemalta. Kouluun tulee myös DALI tekniikalla toteutettu valaistusjärjestelmä, johon kuuluu 30 valaisinreititintä, sekä niiden hallintatyöasema (Liite 3.). Normaaleihin opetusluokkiin tulee 2 Cynap -laitetta, joilla voidaan hallita kahta näyttöä per luokka. Sisältöä täytyy pystyä toistamaan langattoman verkon ylitse. Ruokasaliin tulee 8 Cynap laitetta ja niihin 8 näyttöä, sekä niille oma keskuslaite (Liite 4.). Liikuntasaliin tulee Crestron NVX järjestelmä, johon tulee 8 NVX laitetta sekä hallintalaite (Liite 5.).

Koulun langattoman verkon tulee olla tarpeeksi kattava ja tehokas tarjoamaan yhteyden kaikille oppilaille sekä opettajille. Langattomasti tulee jakaa opetuskäyttöön tarkoitettua verkkoa, johon pääsevät sekä oppilaat että opettajat. Tavoitetilan verkossa myös matkapuhelintaajuudet toimivat sisätiloissa moitteettomasti.

5.4 Saatavuus

Rakennuksen tietoverkon ei tarvitse olla 99% saatavilla. Opetusta voidaan jatkaa koulussa ilman internet yhteyttäkin ja huoltoja ja korjauksia voidaan tehdä koulun ollessa suljettuna. Kuitenkin rakennuksen runkoyhteydet kahdennetaan, eli kaikki kuljetuskerrokselta ylöspäin, mikä lisää toimintavarmuutta järjestelmille huomattavasti. Tietoverkon ruuhkatilanteisiin varaudutaan priorisoimalla järjestelmien liikennettä ruuhkatilanteessa normaalin käyttäjän Internet käytön edelle.

5.5 Kapasiteetti

Tavoitetilan verkossa tulee olla tarpeeksi kaistanleveyttä kuljettamaan oppilaiden sekä opettajien liikenne moitteettomasti. Mitoitukseen on otettava huomioon myös järjestelmien tarvitsemat kaistanleveydet. Kuitenkin etukäteen kaistanleveyden arviointi voi vaihdella hyvin paljon realistisesta määrästä. Tavoitetilan kaistanleveys (etenkin WAN) on mitoitettu siten, että WAN liitännän jatkuva keskiarvokuorma on maksimissaan 40% kaistanleveydestä. Ylimitoitus on kallista, ja alimitoitus johtaa vikatilanteisiin. Tavoitetilassa tähdätään siis mitoittamaan Internet linkki siten, että sen jatkuva keskikuormitus on noin 35%, jolloin se kestää ruuhkatilanteita, mutta ei ole vielä liikaa ylimitoitettu.

5.6 Kaapelointi

Nykykaapelit ovat tehokkaita tiedonsiirtokapasiteetiltaan, joten kaapelointien tulee tukea 10Gbit/s nopeuksia. Silloin kaapeloinnit ovat riittävät, sekä laajentamisen varaa myös löytyy. Matkat ovat otettava huomioon, että kaapelin tukemat etäisyydet eivät ylity.

5.7 Verkkomallin valinta

Tavoitetilan verkkomallin tulee tukea rakennukseen tulevia järjestelmiä sekä sen on oltava laajennettavissa tulevaisuutta ajatellen.

5.8 Internet, etähallinta ja monitorointi

Koulusta tulee lähteä suora internet -yhteys, johon tilataan operaattorilta myös palomuuri, jonka säännöstö tulee olla hallittavissa monitorointia ja etähallintaa varten. Julkisten IP osoitteiden määrä tulee olla mahdollisimman pieni, mutta riittävä vastaamaan etähallittuja palveluita sekä monitorointia.

5.9 Tietoturva

Fyysiseen tietoturvaan on panostettava, esimerkiksi lukitsemalla kaikki laitetilat. Palomuurissa tulee kieltää kaikki liikenne ensin, ja sallia vain tarvittavat. Palomuurisäännöissä tulee käyttää mahdollisimman pieniä verkkomaskeja. Kaikki käytettävät salasanat tulee olla vahvoja, sekä tietoverkon segmentit ovat harkitusti eristettyjä toisistaan loogisella tasolla.

Tavoitetilaan kuuluu olennaisesti tietoverkon käyttäjät, jotka tavoitetilassa ovat tietoisia tietoturvallisuudesta sekä suhtautuvat kriittisesti lähteisiin ja ovat tietoisia sosiaalisesta käyttäjän manipuloinnista.

Tavoitetilan tietoverkossa on varauduttu toimintasuunnitelmin mahdollisiin kyber -hyökkäyksiin ja tiedetään miten toimia ongelman ilmetessä. Myös tietojen häviäminen on otettu huomioon varmuuskopioimalla tärkeä data säännöllisin väliajoin.

6 Tietoverkon suunnittelu tavoitetilaan

Kun tavoitetila on selvillä, lähdetään suunnittelemaan tietoverkkoa vastaamaan tavoitetilan määrityksiä. Tässä kappaleessa suunnitellaan tietoverkko vastaamaan esimerkkitavoitetilan määrityksiä. Tämän tutkimuksen tietoverkkoa ei toteuteta, vaan se toimii esimerkkinä tietoverkon suunnitteluohjeessa.

6.1 Mitoitus ja palvelunlaatu

Tietoverkkoa on hankala mitoittaa vielä tässä vaiheessa, sillä ei vielä tiedetä mihin kytkimiin laitteet fyysisesti sijoitellaan. Siksi liikenne voidaan mitoittaa ja priorisoida jo etukäteen VLAN tasolla, eli loogisella tasolla. Tämä onnistuu jakelukerroksessa, mikäli käytössä olevat kuitukytkimet ovat L3 tason kytkimiä. Liikenne merkataan VLAN leiman mukaisesti, ja liikennettä rajoitetaan tai priorisoidaan sisääntulevassa rajapinnassa. Liikennettä ei tarvitse myöskään rajoittaa, jos ruuhkatilannetta ei ole. Vasta kilpailutilanteessa alemman luokan liikennettä pudotetaan tai viivästetään. Liikennettä voidaan merkata DSCP tai Precedence -luokilla. Tähän verkkoon valittiin Precedence -merkkaukset. Suunniteltaessa liikenteen luokittelua, on tärkeää miettiä mikä liikenne ruuhkatilanteessa on tärkeää, ja mistä voidaan ”verottaa”. Yleensä loppukäyttäjien liikenne eli normaali Internet selailu merkataan huonoimpaan luokkaan. Järjestelmät kuten kulunhallinta ja kameravalvonta merkataan korkeampaan luokkaan, sillä niiden täytyy toimia myös ruuhkatilanteessa. Mietitään siis jokaiselle VLAN verkolle prioriteetti, luokka, ja rajoitus tai ohitussääntö. Aluksi luokitellaan liikenne 0-5 tärkeysasteikolla taulukon 6 mukaisesti.

Taulukko 6 Liikenteen luokittelu

Järjestelmän tai ryhmän nimi	**VLAN**	**Precedence**
Kiinteän verkon Internetliikenne	14	0
Langattoman verkon Internetliikenne	16	0
Ruokalan Cynapit	18	3
Turvakamerat ja tallennin	11	3
Kameroiden monitorointi	12	2
Dali reitittimet ja hallinta	13	4

CP3N Hallintalaite	19	3
Lenel kulunhallinta	20,21	4
Projektorijärjestelmä	22	3

Seuraavaksi mietitään luokille säännöt, jonka mukaisesti liikennettä rajoitetaan tai ohitetaan ruuhkatilanteessa. Oheiset taulukon 7 mukaiset säännöt ovat mietitty 1Gbit/s tietoverkolle ja ne voidaan liittää jakelukerroksen kytkimillä rajapintoihin IN suuntaan, jolloin liikenne merkataan ja rajoitetaan ruuhkatilanteessa jo sisääntulevassa rajapinnassa, jolloin saadaan esimerkiksi työasemien lataus- sekä lähetysliikenne rajoitettua, jos ruuhkatilanne syntyy.

Taulukko 7 Liikenteen rajoitus tai ohitussäännöt

Precedence	**Sääntö ruuhkassa**
0	Salli 50% linkin kapasiteetista, leikkaa loput
1	Ei käytössä
2	Anna 15Mbit/s, leikkaa loput
3	Anna 350Mbit/s, jonota loput
4	Jonon ohi 50Mbit/s

Näillä palvelunlaatu asetuksilla saadaan tietty liikenne kulkemaan myös silloin, jos tietoverkossa on ruuhkaa, koska halutaan esimerkiksi valaistusjärjestelmän, kulunhallinnan sekä kameravalvontaverkon toimivan moitteettomasti.

Operaattoriliitynnän haluttiin olevan noin jatkuvalla 30-35% käyttöasteella, jolloin se ei ole liian yli- tai alimitoitettu. Jatkuvan liikenteen realistiset arvot saadaan vasta sitten kun tietoverkko on käyttöönotettu ja sitä on monitoroitu ja mitattu ainakin kaksi kuukautta. Operaattoriliitynnän nopeudeksi voidaan valita käyttöönotossa 1Gbit/s, ja nostaa tai laskea nopeutta seurannan jälkeen. Operaattoriliitynnän on oltava kuituliitynnällä.

6.2 Kaapelointi

Tietoverkon kaapeleiksi valitaan kuitukaapelia, sekä kuparia. Liityntäverkon laitteet yhdistetään kytkimiin Cat6A luokan kuparilla, sillä sen tiedonsiirtonopeus on todella hyvä hintaan verrattuna. Kaapeleissa käytetään U/FTP suojausta interferenssin minimoimiseksi. Runkokaapeloinnissa käytetään OS2 -luokan yksimuotokuitua sekä OM3 -luokan monimuotokuitua, riippuen yhteyden välimatkasta.

6.3 Tietoturva

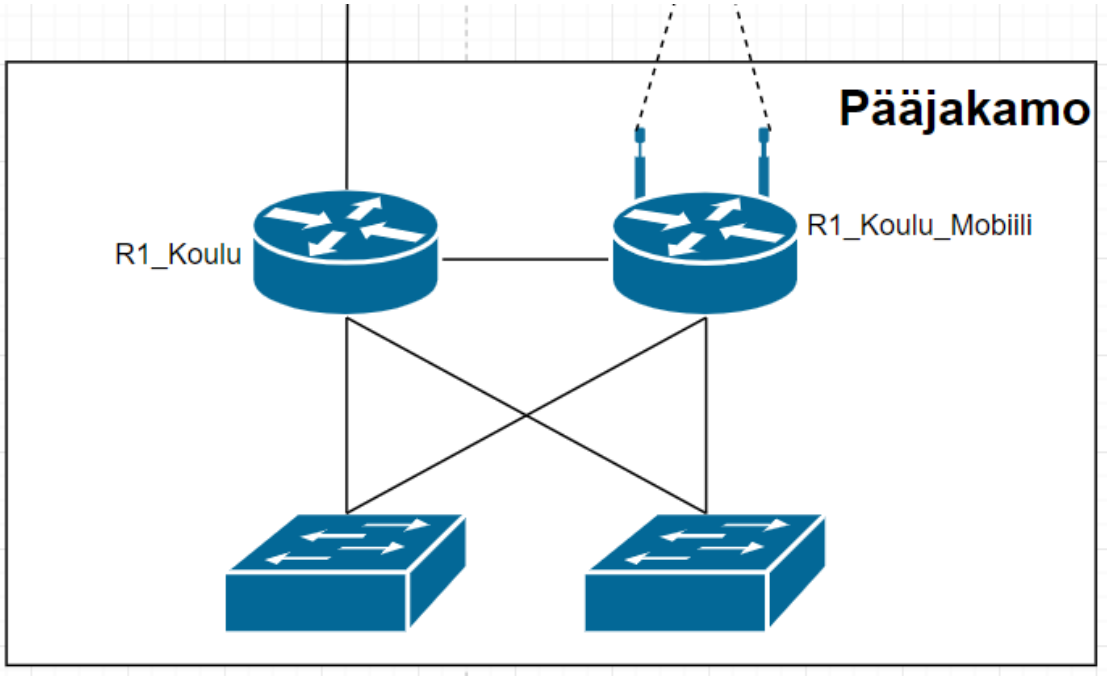
Fyysiseen tietoturvaan varaudutaan pitämällä laitekaapit ja laitehuoneet lukittuina. Tietoverkon sisäistä tietoturvaa ylläpidetään jakamalla verkon osa-alueet virtuaalisiin aliverkkoihin, joista oikeudet muihin verkkoihin ovat rajatut. Tietoverkossa kulkevaa liikennettä monitoroidaan ja poikkeavat liikennevirrat selvitetään. Palomuurista sallitaan vain ne portit, joita tarvitaan. Lisäksi tietoverkon laitteiden lisenssit ja ohjelmistot on pidettävä ajan tasalla. Rakennuksen henkilökunnalle voidaan pitää lyhyitä koulutuksia tietoturvallisuudesta.

Tietoverkon ylläpitäjällä tulisi olla suunnitelma, mitä tehdä mahdollisen kyberhyökkäyksen alla. Esimerkiksi palvelunestohyökkäyksiin voidaan tehdä toimintaohje jo etukäteen. Suunnitelmassa tulee miettiä pahimpia tilanteita ja pyrkiä varautumaan niihin.

6.4 Saatavuus ja kahdennukset

Kuten esimerkkitavoitetilassa määriteltiin, ei tietoverkon tarvitse olla korkeasti saatavilla, mutta siihen halutaan kuitenkin mahdollisimman paljon toimintavarmuutta. Lii-

tyntäverkon laitteet yhdistetään kahdennettuihin jakeluverkon laitteisiin, ja operaattoriliityntään halutaan varayhteys. Varayhteys takaa sen, että linjan tai reitittimen hajotessa yhteys saadaan varayhteyden kautta. Varayhteyttä ei voi koskaan asentaa samaan kaapeliin pääyhteyden kanssa. Koululle tulee vain yksi kuitu tässä tapauksessa, joten varayhteydeksi valitaan mobiilireititin ratkaisu, jolloin toista kaapelia ei tarvitse vetää ja säästetään rahaa. Varalinjan mobiilireitittimessä on sama konfiguraatio kuin pääreitittimessä, jolloin verkon toiminta pysyy päälinjan katkoksen aikana täysin samana. Pääjakamoon tulee siis kuvion 24 mukaiset laitteet, kuitenkin jakeluverkon kuitukytkimiä voi olla enemmän.



Kuvio 24 Pääjakamon varmennettu operaattoriliityntä sekä laitteet

6.5 Monitorointi

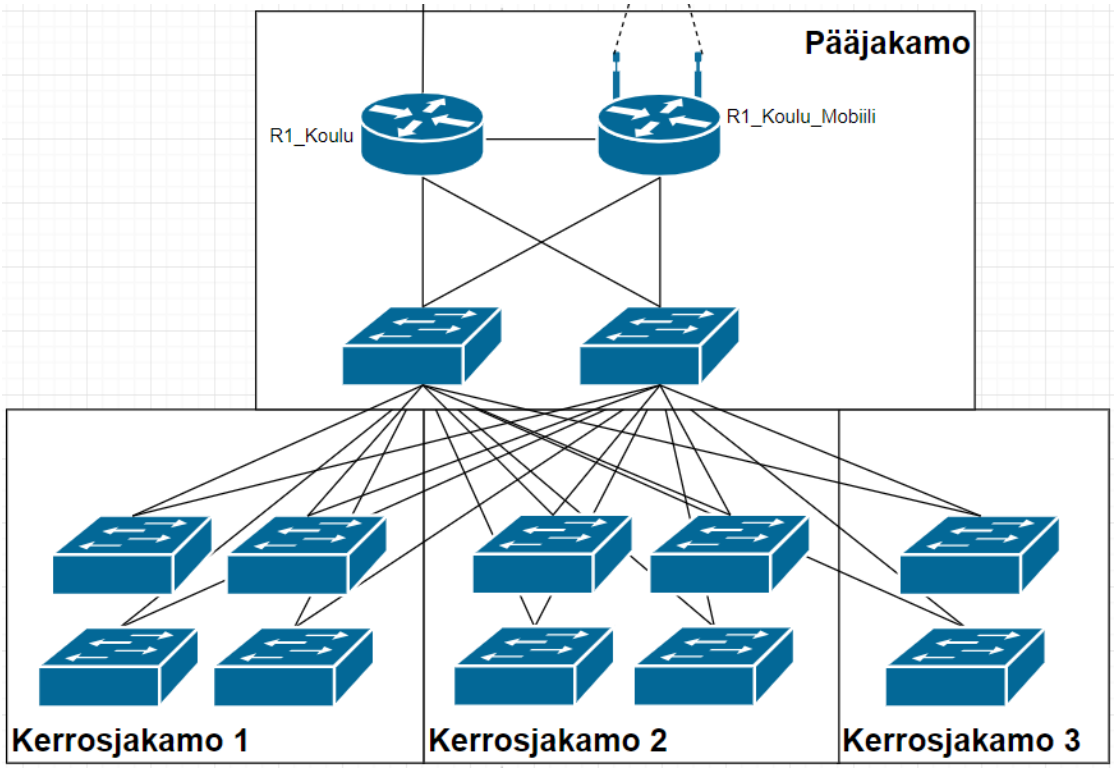
Tietoverkon ylläpitäjä on vastuussa verkon monitoroinnista. Monitorointiin on saatavilla paljon erilaisia hyviä työkaluja. Tässä tutkimuksessa ei avata monitoroinnin konfiguraatiota tai toteuttamista laajasti. Tietoverkon monitoroinnilla tulee pystyä seuraamaan verkossa kulkevia liikennemääriä ja havaitsemaan poikkeamia normaalista. Monitorointiin kuuluu lokien tallennus ja seuraaminen, joista hälytykset suodatetaan

ja vikatilanteisiin puututaan mahdollisimman nopeasti. Kaikki verkon aktiivilaitteet tulee olla seurannassa, jolloin mahdolliset viat saadaan rajattua mahdollisimman nopeasti. Monitorointityökalun tulee olla selkeä lukuinen ja tietoverkossa tulee olla riittävästi sensoreita, joista dataa voidaan tarkistella.

6.6 Fyysiset verkkokuvat

6.6.1 Koulun fyysinen runkoverkko

Fyysiseen verkkokuvaan kuvataan laitteistot ja kaapeloinnit juuri sellaisena kuin ne tulevat olemaan. Jos käyttöönoton yhteydessä tai muulloin tehdään muutoksia, on muutokset muutettava aina verkkokuvaan. Verkkokuvasta tulee käydä ilmi myös rajapinnat laitteiden välillä sekä laitteiden sijainti. Tässä tutkimuksessa sijaintia laitteille ei kuvata sillä verkkosuunnittelu on esimerkki. Liitteistä 1-8 voidaan laskea, montako laitetta tarvitsee vapaan kytkimen portin koululta huomioiden, että Crestron NVX järjestelmään tulee täysin oma kytkin, joten niitä ei lasketa mukaan. Lukemaksi saadaan 223 laitetta. Jos esimerkiksi valituissa liityntäkytkimissä olisi 24 Ethernet porttia sekä 2 Uplink kuituporttia, 11 kytkintä riittäisi kaikille laitteille. Portteja on silloin käytössä 242 joista käyttöön tulee ainakin 223. Kun 11 liityntäkytkintä yhdistetään kuidulla jakeluverkon kuitukytkimiin, niin jakeluverkon kytkimeen tulee käyttöön silloin 22 kuituporttia liityntäkytkimille, ja 2 Uplink -porttia reitittimien yhdistämiseen. Koulun aktiivilaitteiden fyysinen verkkokuva nähdään kuviossa 25, jossa kaikki piuhat ovat kuitukaapelia.



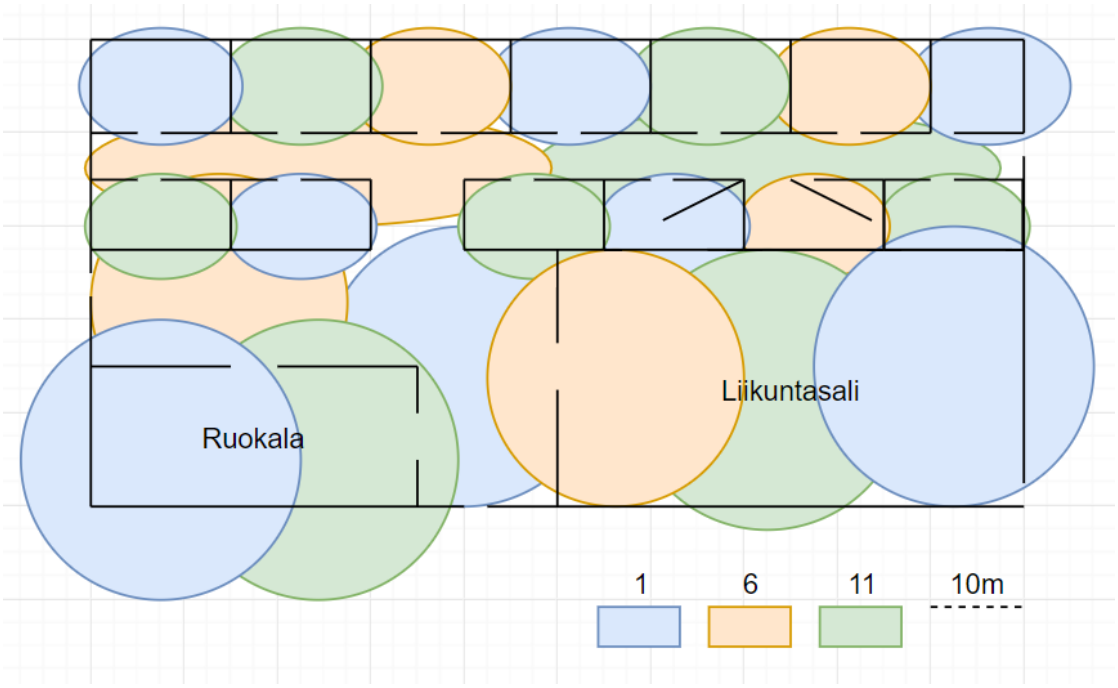
Kuvio 25 Koulun runkoverkon topologia

Verkkoon liitettävät palvelimet, monitorointityöasemat, kamerat tai monet muut laitteet voidaan yhdistää mihin tahansa näistä kytkimistä. Kytkennät huomoidaan konfiguroitaessa kytkimiä.

6.6.2 Langaton verkko ja kanavajako

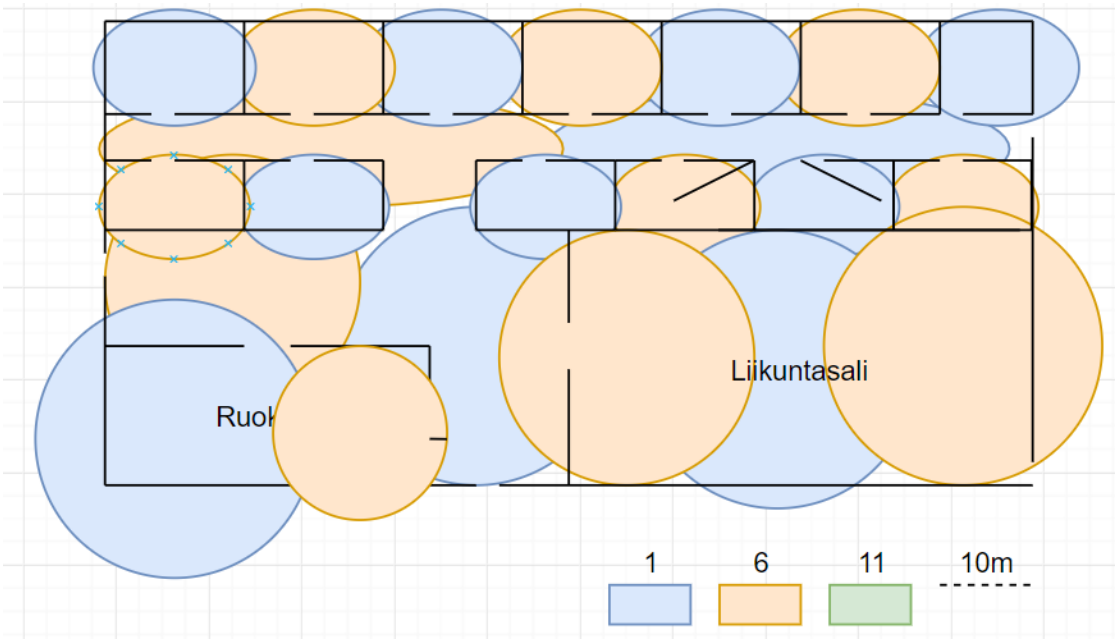
Rakennukseen on kuvitteellisesti valittu tukiasemat, joiden signaalin ympärisäteilevä kantavuus on noin 20 metriä tukiasemasta jokaiseen suuntaan. Tukiasemia sijoitetaan siis siten, että signaaleille saadaan hieman päällekkäisyyttä. Näin vältetään signaalittomat kohdat verkossa. Jokaiseen luokkaan sijoitetaan oma tukiasema. Lähetysteho on säädettävä luokkien tukiasemissa mahdollisimman pieneksi siten, että yhteys luokassa toimii, mutta signaali kuuluu luokan ulkopuolelle heikosti, jotta saadaan häiriöt minimoitua luokan ulkopuolisten signaalien kanssa. 5 Ghz:n Opetusverkko voi tässä tapauksessa olla automaattisella kanava-asetuksella, koska sillä ei pitäisi häiriöitä syntyä. Kuviossa 26 nähdään rakennuksen 2.4 Ghz:n kanavasuunnittelu. Pitkillä

käytävillä käytetään erilaista antennia, joka antaa pitkittäisen peittokuvion häiriöiden minimoimiseksi, sekä peittämään pitkän käytävän vain kahdella tukiasemalla.



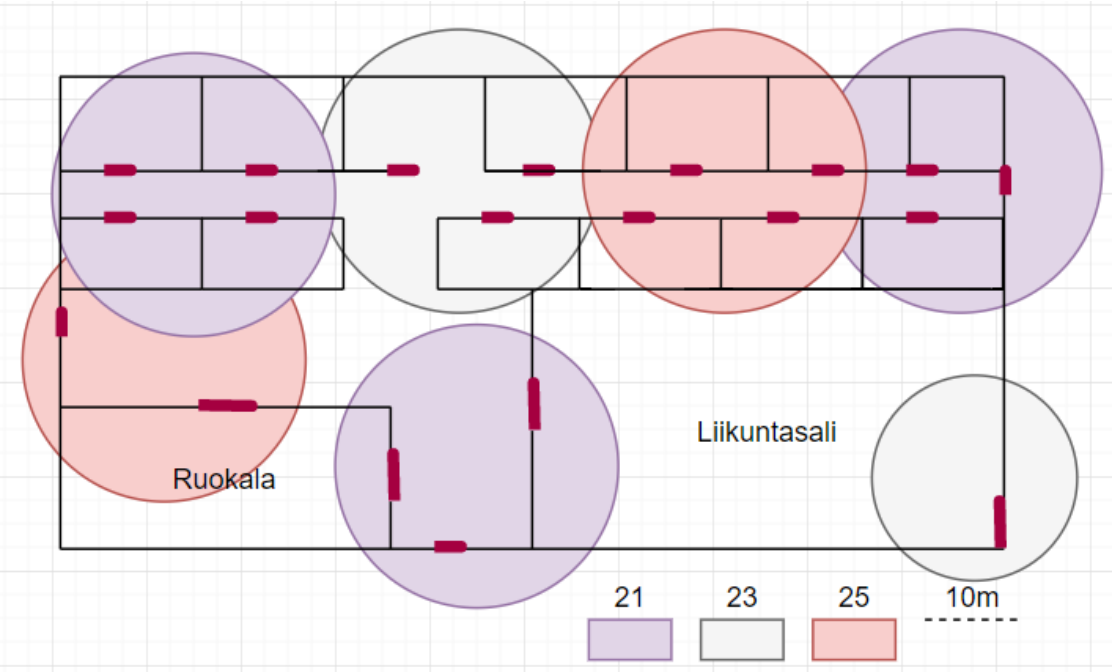
Kuvio 26 2.4Ghz Kanavasuunnitelma

Kuitenkin ongelmaksi tässä toteutuksessa tulee se, että mukaan pitäisi vielä saada Aperio Hubit, jotka jakavat myös 2.4Ghz taajuuksilla signaaleja langattomille lukoille. Käytännössä sovittaminen mukaan olisi lähes mahdotonta, joten ratkaisuksi jätettiin 2.4Ghz opetusverkosta kanava 11 käyttämättä, jolloin kaikki Hubit voivat käyttää kanavia 21-26, jotka eivät mene toistensa päälle, eivätkä silloin ota häiriöitä ollenkaan 2.4Ghz opetusverkosta. Hubeilla voidaan käyttää varmuuden vuoksi jokatoista kanavaa, esimerkiksi 21, 23 ja 25 kanavia. Suunnitelman mukainen opetusverkon kanavajako näyttäisi silloin kuvion 27 mukaiselta.



Kuvio 27 Langaton opetusverkko ilman kanavaa 11

Tässä toteutuksessa tärkeää on tukiasemien lähetystehojen huomioiminen. Lähetystehot on syytä mitata ja säätää käyttöönoton yhteydessä. Kuitenkin tämä jako on hyvä sillä se takaa langattomien lukkojen toiminnan. 2.4Ghz:n Opetusverkkoa ei muutenkaan kannata käyttää, vaan oppilaiden ja opettajien on syytä yhdistää aina 5.0 Ghz:n verkkoon, joka on nopeampi, sillä tällä toteutuksella on aina näköyhteys tukiasemaan. 2.4Ghz opetusverkko kuitenkin jaetaan sillä kaikki päätelaitteet eivät vielä tue 5.0Ghz:n taajuuksia. Tähän jakoon Aperio Hubien sijoittelu ja suunnittelu on helppoa, kun 2.4Ghz verkkoa ei enää oteta suunnittelussa huomioon. Yksi Aperio Hub tukee 8 lukkoa ja signaalin kantama on noin 20 metriä, joten suunnitellaan Hubit 30 metrin välein kuvion 28 mukaisesti. Kuvion mukaiset lukot konfiguroidaan sen päällä olevalle kanavalle.



Kuvio 28 Aperio Hubien kanavasuunnittelu

6.6.3 Aktiivitoistimet

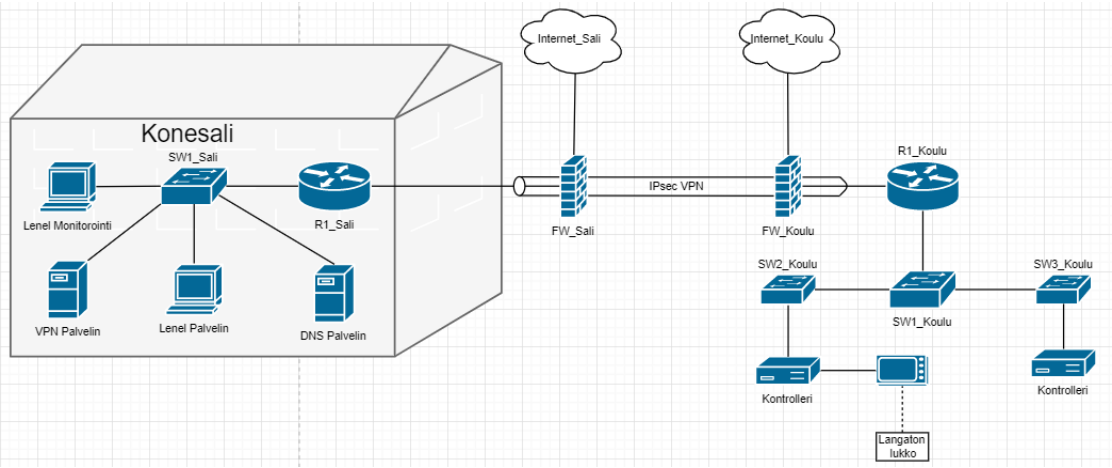
Uudet rakennukset ovat usein tehokkaita vaimentamaan mobiiliverkon signaaleja sisätiloissa. Tästä syystä rakennuksiin voidaan operaattorin toimesta tuoda aktiivitoistin -laitteet, jotka toistavat mobiiliverkon taajuuksia sisätiloissa. Toistimilla saadaan matkapuhelinverkko kuulumaan myös sellaisissa tiloissa, joita matkapuhelinverkko ei läpäise hyvin. Toistimet voivat olla yhden operaattorin toistimia, tai monioperaattoriratkaisuita. Monioperaattoritoistin -järjestelmä toistaa monen eri operaattorin matkapuhelintaajuuksia. Tämä saa suuren osan henkilöistä käyttämään päätelaitteita matkapuhelinverkossa, jolloin langattomalta Wifi -verkolta tippuu kuormaa. Suosituksena siis on rakentaa monioperaattoritoistin -järjestelmä rakennukseen.

6.7 Loogiset verkkokuvat ja osoitteistus

Loogiset verkkokuvat hahmotellaan vastaamaan järjestelmävaatimuskortteja. Verkkokuvien lisäksi järjestelmät osoitteistetaan ja aliverkotetaan. Loogisissa verkkokuvissa fyysinen topologia voi olla yksinkertaistettu, mutta järjestelmän toiminnallisuus tulee käydä ilmi kuvista.

6.7.1 Lenel -järjestelmän looginen verkkokuva ja osoitteistus

Lenel -järjestelmän pääpalvelin on virtualisoitu konesaliin, jossa sijaitsee myös koulun virtualisoitu DNS -palvelin. Konesalista on IPsec VPN -tunneli suoraan koulurakennuksen reitittimelle, mikä luo konesalista osan sisäverkkoa, jolloin kontrollerit ja Lenel -palvelin eivät tarvitse Internet -yhteyttä keskustellakseen. Järjestelmää voidaan hallita ja monitoroida etänä monitorointi työasemalta, joka on myös virtualisoitu konesaliin. Monitorointi asemalle pääsee kiinni RDP yhteydellä, ainoastaan silloin kun käyttäjä on ensin avannut yhteyden konesalissa sijaitsevalle VPN palvelimelle, johon käyttäjä voi kirjautua mistä tahansa Internet -yhteydellä. Verkkokuvaan ei kuvata kaikkia lukkoja tai Hubeja, sillä ne eivät keskustele IP:n ylitse, joten ne eivät ole olennainen osa verkkokuvaa. Järjestelmä on kuvattu kuvioon 29.



Kuvio 29 Lenel -järjestelmän looginen verkkokuva

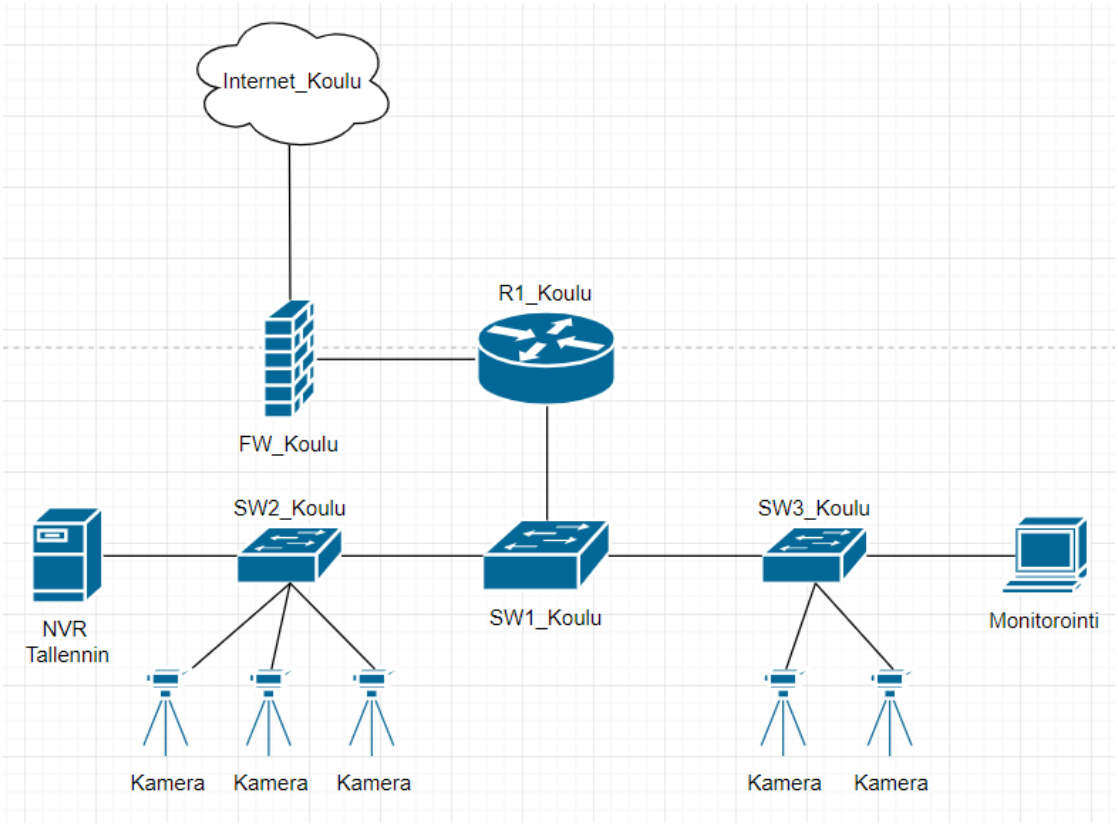
Lenel -järjestelmä konfiguroidaan staattisin IP osoittein, taulukon 8 mukaisesti.

Taulukko 8 Lenel -järjestelmän osoitteistus

Laitteen nimi	**VLAN**	**Verkko-osoite**	**IP-osoite**	**Gateway**
Lenel Monitorointi	20	192.168.20.0/24	192.168.20.10	192.168.20.1
Lenel Palvelin	20	192.168.20.0/24	192.168.20.20	192.168.20.1
Kontrolleri1	21	192.168.21.0/24	192.168.21.10	192.168.21.1
Kontolleri2	21	192.168.21.0/24	192.168.21.20	192.168.21.1

6.7.2 Kameravalvontajärjestelmän looginen verkkokuva ja osoitteistus

Kameravalvontajärjestelmä on oma virtuaalinen aliverkkonsa, josta ei ole pääsyä internettiin, eikä sille konfiguroida DHCP:tä. Aliverkkoon kuuluu myös NVR tallennin. Kamerat streamaavat kuvansa tallentimelle, joka sijaitsee myös koululla fyysisesti. NVR tallennin on paikallisessa lähiverkossa, sillä kameroiden kuorma on WAN linkillä kallista, joten on parempi pitää lähetykset sisäverkossa. Monitorointi työasema ei kuulu samaan aliverkkoon, sillä sille halutaan myös Internet pääsy ja NAT, joten on turvallisempaa pitää se erillään kameroiden aliverkosta. Monitorointi PC:lle sallitaan pääsy kuitenkin kameroiden aliverkkoon, jotta se pääsee katselemaan kameroita NVR tallentimen nettikäyttöliittymästä. Kameraverkkoon sallitaan pääsy siis vain monitorointi PC:n aliverkosta. Järjestelmä on kuvattu kuvioon 30.



Kuvio 30 Kameravalvontajärjestelmän looginen verkkokuva

Kameravalvontajärjestelmälle suunnitellut osoitteistukset nähdään taulukossa 9.

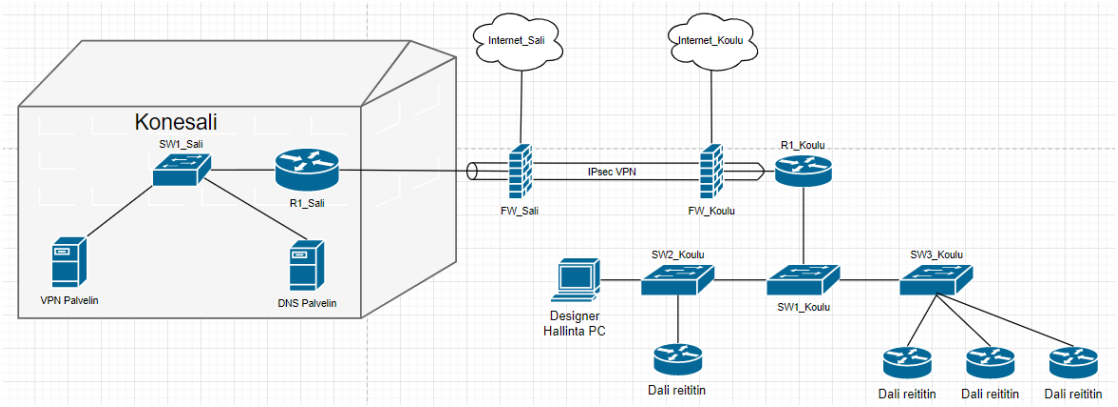
Taulukko 9 Kameravalvontajärjestelmän osoitteistus

Laitteen nimi	**VLAN**	**Verkko-osoite**	**IP-osoite**	**Gateway**
Turvakamerat	11	192.168.11.0/24	192.168.11.2-16	192.168.11.1
NVR Tallennin	11	192.168.11.0/24	192.168.11.20	192.168.11.1
Monitorointi PC	12	192.168.12.0/30	192.168.12.2	192.168.12.1
R1_Koulu g0/0/0.11	11	192.168.11.0/24	192.168.11.1	
R1_Koulu g0/0/0.12	12	192.168.12.0/30	192.168.12.1	

6.7.3 Valaistusjärjestelmän looginen verkkokuva ja osoitteistus

Valaistusjärjestelmään kuuluu 30 Dali -reititintä, sekä yksi hallintaohjelmalla varustettu PC. Järjestelmä on toteutettu yhdellä työryhmällä eli VLAN:illa, koska siihen

kuuluu vain 30 reititintä. Yksi VLAN kestää noin 100 reititintä, joten on yksinkertaisempaa pitää reitittimet samassa VLAN:issa tässä tapauksessa. Hallinta PC sijaitsee koulussa, eikä siinä ole Internet yhteyttä. Hallinta PC:lle kuitenkin voi ottaa etäyhteyden VPN palvelimen kautta, joka sijaitsee konesalissa. Kokojärjestelmä osoitteistetaan kiinteillä privaateilla IP osoitteilla. Kaikkia Dali -reitittimiä ei hahmoteltu kuviossa 31.



Kuvio 31 Valaistusjärjestelmän looginen verkkokuva

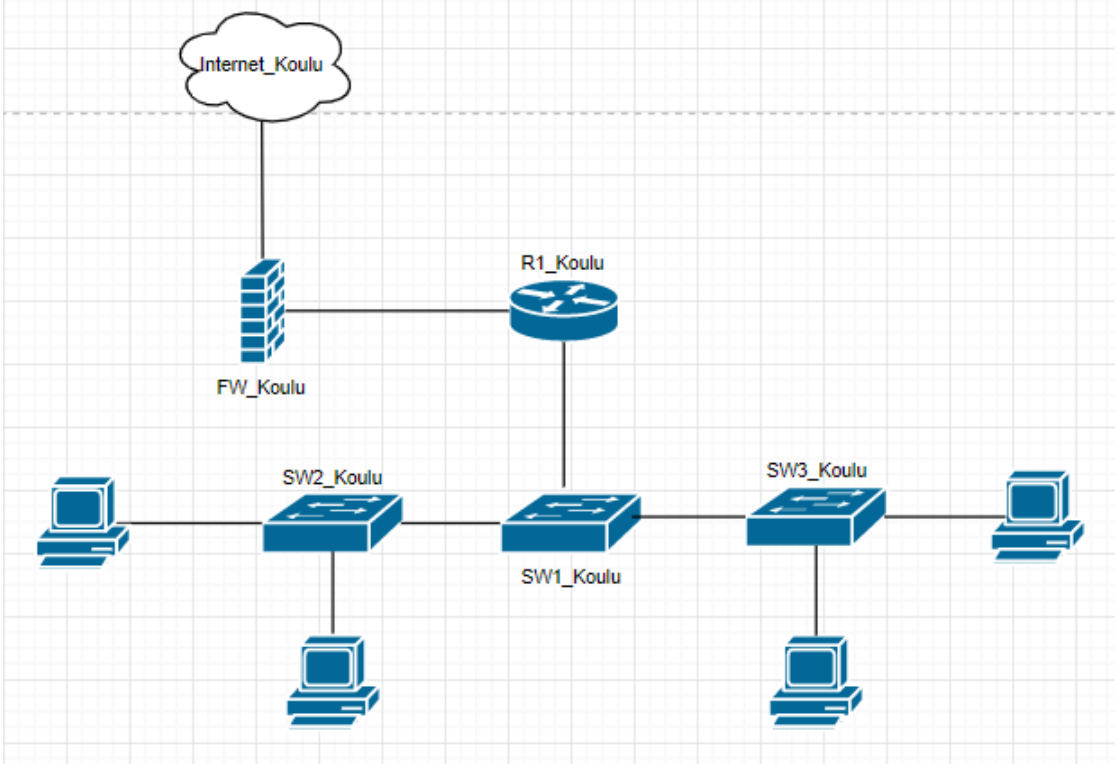
Valaistusjärjestelmälle annetaan isompi osoiteavaruus, sillä sitä pilkotaan ohjelmallisesti pienempiin ryhmiin. Pilkkomisessa käytetään IP osoitteen C-luokkaa, joten valaistusreitittimille(taulukko 10) annetaan /21 maskin avaruus, josta riittää jaolle hyvin osoitteita.

Taulukko 10 Valaistusjärjestelmän osoitteistus

Laitteen nimi	**VLAN**	**Verkko-osoite**	**IP-osoite**	**Gateway**
Dali -reititin	13	10.0.0.0/21	10.0.1-7.1-254	10.0.0.1
Designer hallinta PC	13	10.0.0.0/21	10.0.0.10	10.0.0.1
R1_Koulu g0/0/0.13	13	10.0.0.0/21	10.0.0.1	

6.7.4 Kiinteän opetusverkon looginen verkkokuva ja osoitteistus

Kiinteä opetusverkko on opetus- ja oppilaskäyttöön tarkoitettu verkko, jonka tehtävänä on tarjota Internetyhteys, sekä pääsy opetusverkon resursseihin. Kuitenkin verkosta on melko rajoitetut oikeudet. Osoitteiden jako (taulukko 11) sekä osoitteiden muunnokset tehdään R1_Koulu -reitittimellä, ja liikenne Internettiin kulkee palomuurin kautta. Verkkokuva nähdään kuviossa 32, johon kuitenkaan kaikkia työasemia (100) ei kuvattu.



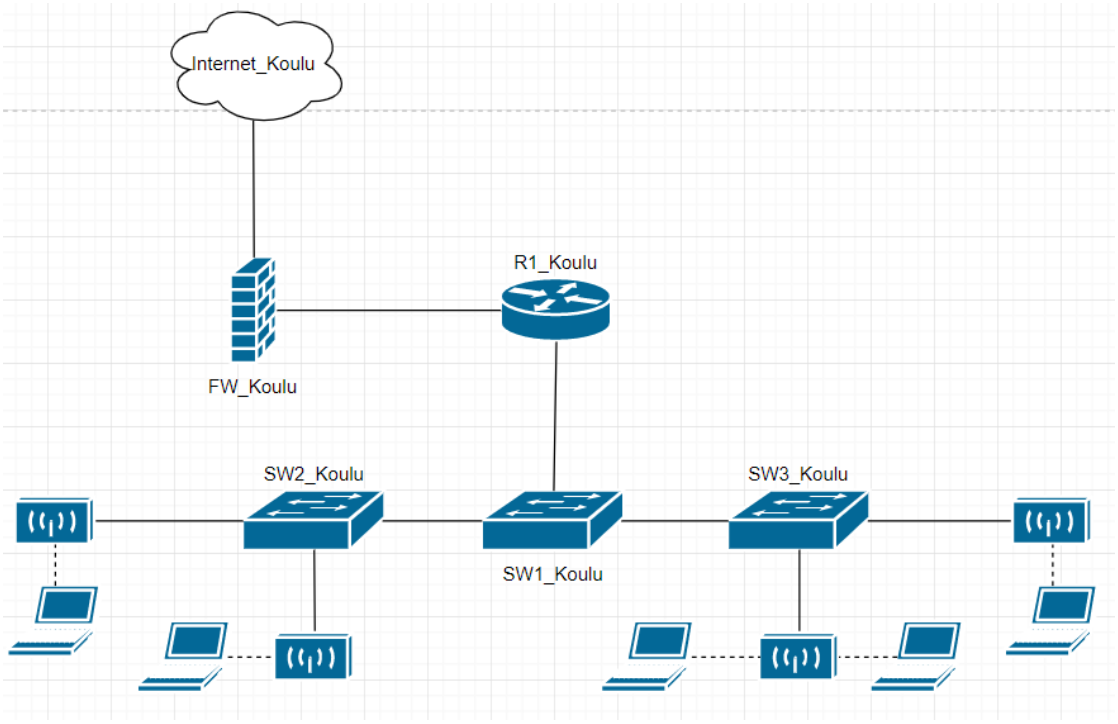
Kuvio 32 Kiinteän opetusverkon looginen verkkokuva

Taulukko 11 Kiinteän opetusverkon osoitteistus

Laitteen nimi	**VLAN**	**Verkko-osoite**	**IP-osoite**	**Gateway**
Kiinteän verkon PC	14	192.168.14.0/24	192.168.14.2-254	192.168.14.1
R1_Koulu g0/0/0.14	14	192.168.14.0/24	192.168.14.1	

6.7.5 Langattoman verkon looginen verkkokuva ja osoitteistus

Langaton verkko tarjoaa Internet yhteyden oppilaille sekä opettajille, sekä pääsyn opetusverkon resursseihin. Langaton verkko mitoitetaan tukemaan ainakin 400 laitetta. Tukiasemat siltaavat liikenteen tietoverkkoon, sekä ne antavat oikeat VLAN leimat SSID:ille. Vastaanottava kytkimen portti on konfiguroitava Trunk -tilaan, vastaanottamaan leimattu liikenne. Tukiasemat jakavat Opetusverkkoa 2.4 Ghz sekä 5 Ghz taajuuksilla, johon pääsevät oppilaat sekä opettajat. Verkko tarjoaa Internet yhteyden, mutta sieltä on rajatut oikeudet. Liikenne Internettiin kulkee palomuurin kautta ja kaikki liikenne Internetistä kielletään. Kuviossa 33 nähdään verkon rakenne, ja selkeyden vuoksi siihen ei laitettu kaikkia päätelaitteita tai tukiasemia.



Kuvio 33 Langattoman verkon looginen verkkokuva

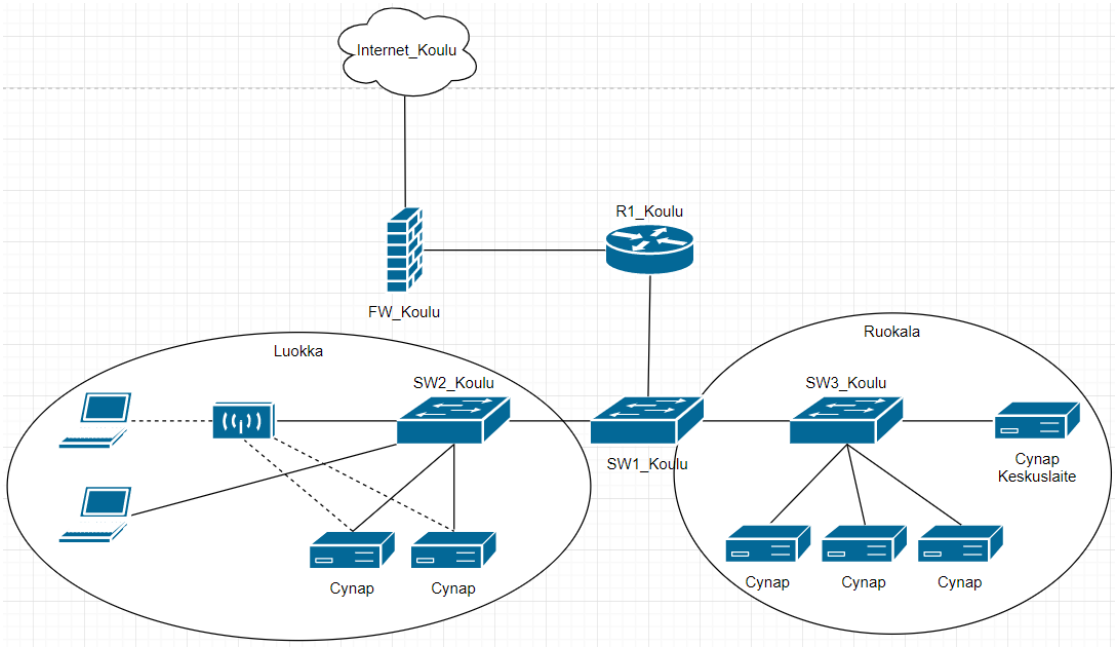
Rakennuksessa on sen verran ihmisiä, että voidaan toteuttaa yhden aliverkon toteutus (Taulukko 12). Isommissa verkoissa verkko täytyy jakaa useampaan Broadcast liikenteen rajaamiseksi. Reititin R1_Koulu jakaa osoitteet DHCP:llä ja toteuttaa osoitteenmuunnokset liikenteen kulkiessa Internettiin.

Taulukko 12 Langattoman verkon osoitteistus

Laitteen nimi	**SSID**	**VLAN**	**Verkko-osoite**	**IP-osoite**	**Gateway**
Tukiasema	Opetus	16	192.168.16.0/23	192.168.16-17.2-254	
Päätelaite		16	192.168.16.0/23	192.168.16-17.2-254	192.168.16.1
R1_Koulu g0/0/0.16		16	192.168.16.0/23	192.168.16.1	

6.7.6 Cynap AV -järjestelmän looginen verkkokuva ja osoitteistus

Cynap -laitteet liitetään langattomaan Opetusverkkoon, sekä kiinteään verkkoon, eli luokkien laitteita käytetään Infrastructure tilassa. Silloin laitteet löydetään ja niitä voidaan käyttää sekä langattomasta, että kiinteästä verkosta. Ruokalan laitteisiin ei haluta pääsyä, sillä niissä halutaan toistaa sisältöä, jota oppilaat eivät voi muokata. Niille annetaan siis oma verkkonsa ja ne yhdistetään ainoastaan kiinteään verkkoon sekä Internettiin. Yksi esimerkkiluokka sekä ruokala on hahmoteltu kuviossa 34. Kaikkia (8) ruokalan Cynappeja ei ole kuviossa.



Kuvio 34 Cynap AV -järjestelmän looginen verkkokuva

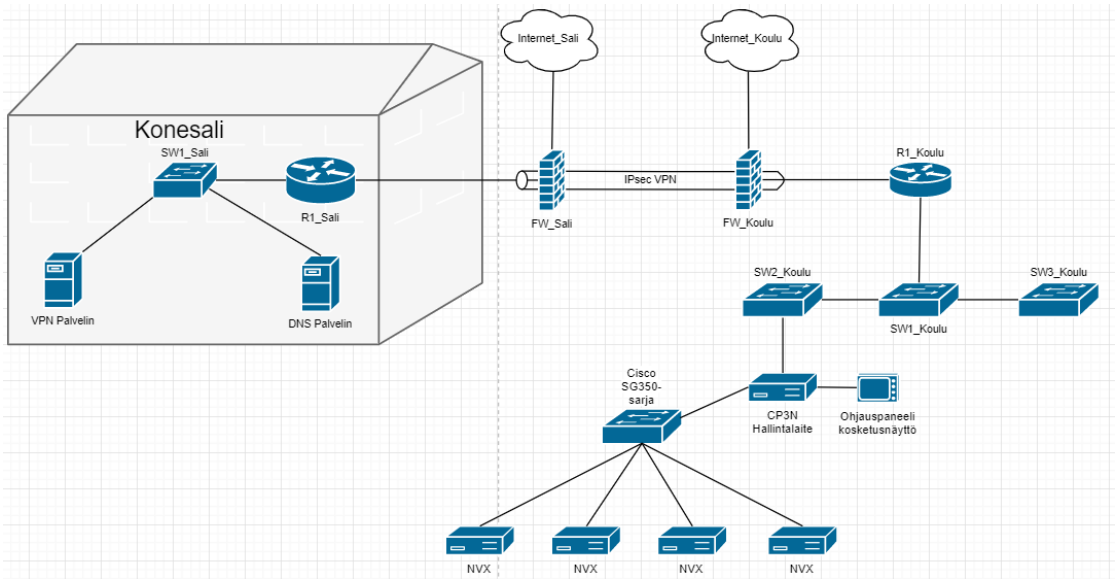
Kuten taulukosta 13 huomataan, luokkien Cynapit liittyvät kiinteään sekä langattomaan opetusverkkoon, ja ruokalan Cynapeille on oma verkkonsa.

Taulukko 13 Cynap AV -järjestelmän osoitteistus

Laitteen nimi	**VLAN**	**Verkko-osoite**	**IP-osoite**	**Gateway**
Cynap_luokka_langa-ton	16	192.168.16.0/23	192.168.16-17.2-254	192.168.16.1
Cynap_luokka_kiinteä	14	192.168.14.0/24	192.168.14.2-254	192.168.14.1
Cynap_ruokala	18	192.168.18.0/24	192.168.18.2-254	192.168.18.1
Päätelaite_langaton	16	192.168.16.0/23	192.168.16-17.2-254	192.168.16.1
Päätelaite_kiinteä	14	192.168.14.0/24	192.168.14.2-254	192.168.14.1
R1_Koulu g0/0/0.14	14	192.168.14.0/24	192.168.14.1	
R1_Koulu g0/0/0.16	16	192.168.16.0/23	192.168.16.1	
R1_Koulu g0/0/0.18	18	192.168.18.0/24	192.168.18.1	

6.7.7 Crestron NVX -järjestelmän looginen verkkokuva ja osoitteistus

NVX Järjestelmä on ”Private Network” tilassa, eli NVX -laitteet eivät juttele kiinteään sisäverkkoon ollenkaan vaan ovat omassa eristetyssä verkossa. Niille osoitteet jakaa CP3N -laite. CP3N liitetään sisäverkkoon ja sen kautta päästään hallinnoimaan järjestelmää. Kuitenkaan emme halua kaikille pääsyä järjestelmään, joten CP3N laitteelle on oma verkkonsa, johon pääsee vain VPN yhteyden kautta. Järjestelmällä ei ole Internet yhteyttä. NVX -laitteet yhdistää Ciscon SG350 sarjan kytkin, joka on testattu ja todettu toimivaksi NVX kytkimeksi. Hallintalaitteeseen yhdistetyllä kosketusnäytöllä voidaan myös hallita järjestelmää.



Kuvio 35 Crestron NVX -järjestelmän looginen verkkokuva

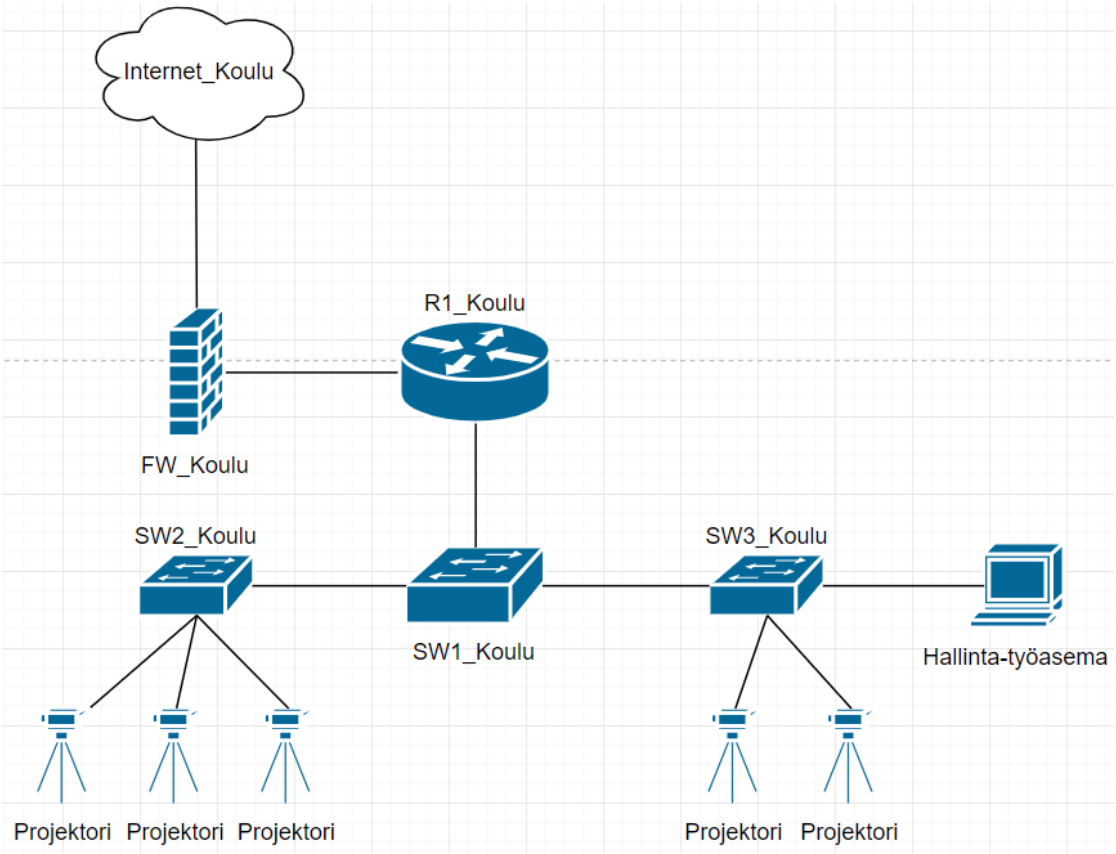
NVX Laitteiden osoitteet voivat olla mitä tahansa, sillä ne eivät kuulu sisäverkkoon millään lailla. Multicast lähetykset pysyvät NVX verkossa. Hallintalaitteelle kuitenkin varataan oma verkkonsa staattisella osoitteella sekä DNS nimellä, jotta VPN kautta päästään helposti hallitsemaan järjestelmää. Koska järjestelmä on Private Network tilassa, osoitteistus pysyy yksinkertaisena taulukon 14 mukaisesti.

Taulukko 14 Crestron NVX -järjestelmän osoitteistus

Laitteen nimi	VLAN	Verkko-osoite	IP-osoite	Gateway
CP3N Hallintalaite	19	192.168.19.0/30	192.168.19.2	192.168.19.1
R1_Koulu g0/0/0.19	19	192.168.19.0/30	192.168.19.1	

6.7.8 Projektorijärjestelmän looginen verkkokuva ja osoitteistus

Rakennukseen tulevat projektorit yhdistetään yleiskaapelointiverkkoon (Kuvio 36). Niille luodaan oma virtuaalinen verkko, johon annetaan pääsyoikeus langattomasta opetusverkosta sekä kiinteästä verkosta. Hallintaohjelmisto voi olla asennettuna mille tahansa tietokoneelle sisäverkossa, ja sieltä voidaan hallita projektoreita keskitetysti.



Kuvio 36 Projektorijärjestelmän looginen verkkokuva

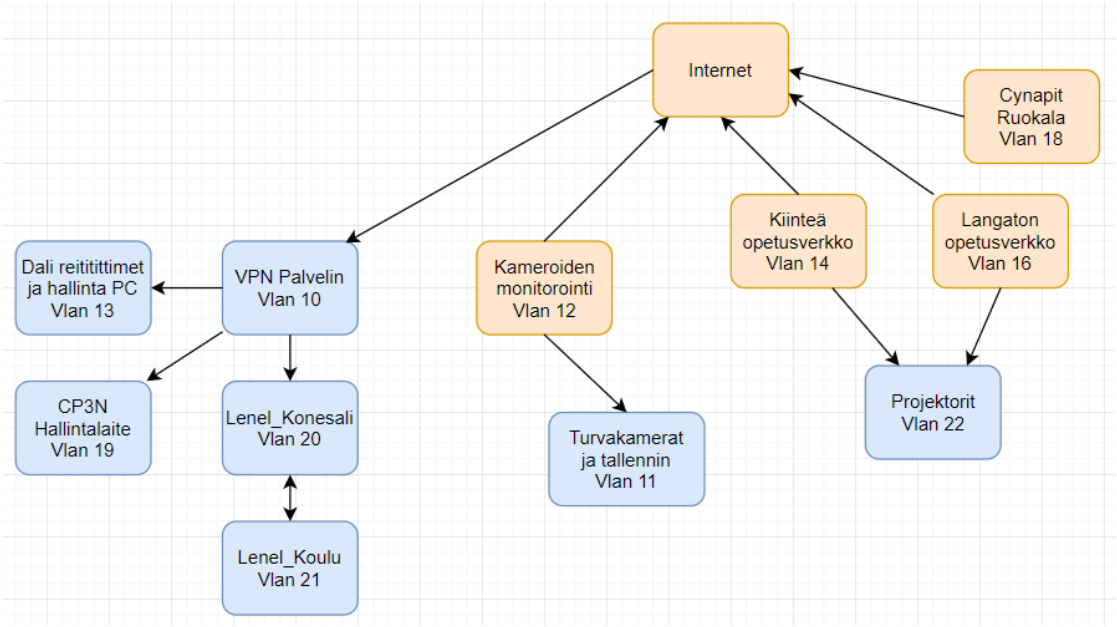
Projektoreille annetaan staattiset IP-osoitteet ja oma virtuaalinen verkko (Taulukko 15), jolloin laitteiden nimeäminen ja määritys helpottuu. Hallintaohjelmiston sisältävä tietokone voi olla joko kiinteässä tai langattomassa verkossa.

Taulukko 15 Projektorijärjestelmän osoitteistus

Laitteen nimi	VLAN	Verkko-osoite	IP-osoite	Gateway
Projektori	22	192.168.22.0/24	192.168.22.2-254	192.168.22.1
R1_Koulu g0/0/0.22	22	192.168.22.0/24	192.168.22.1	

6.7.9 Verkkojen pääsyoikeudet ja rajoitukset

Pääsyoikeuksia tulee miettiä tarkasti, että mistä verkosta voidaan jutella minnekin, ja mistä ei haluta liikenteen kulkevan. Verkkojen välistä liikennettä voidaan rajoittaa esimerkiksi Access -listoilla. Pääsyoikeuksia voi miettiä helpoiten visualisoimalla verkot ja komponentit, ja piirtämällä sellaiset liikennevirrat, jotka on sallittava. Kaikki liikennevirrat, joita ei ole piirretty, kielletään. Kuviossa 37 nähdään koulun verkkojen liikennevirrat visualisoituna. Kuviossa Internet liikennettä sisältävät verkot ovat oranssilla ja vain sisäverkon aliverkot ovat sinisellä.



Kuvio 37 Virtuaalisten verkkojen väliset yhteydet

7 Pohdinta

7.1 Tutkimuskysymys ja sen tulokset

Tutkimuksen tavoitteena oli luoda sellainen tietoverkon suunnitteluohje, jolla voidaan parantaa taloteknisten järjestelmien toimintavarmuutta ja poistaa aiemmin esiintyneitä ongelmia. Tutkimuksen tuloksena saatiin tuotettua alustava verkkosuunnitteluohje, joka keskittyy erityisesti talotekniikkajärjestelmien toimintaan tietoverkon näkökulmasta. Ongelmia aiemmista ratkaisuista löydettiin haastattelemalla alan asiantuntijoita ja tarkistelemalla aiempia toteutuksia. Näihin ongelmiin pyrittiin keskittymään luomalla tietoverkon esimerkki suunnitelma vastaamaan tavoitetilaa. Ratkaisuihin päästiin, mutta sillä ratkaisuita ei testattu käytännössä on vaikea arvioida, vaikuttiko toteutusohje järjestelmien toimintaan positiivisesti. Tutkimuskysymykseen ei siis päästy vielä faktapohjaisesti vastaamaan, vain pelkästään teoriatasolla.

7.2 Ratkaisuiden analysointi

Onnistuttiin luomaan alustava ohje suunnittelulle ja yksi esimerkkitoteutusratkaisu. Onnistuttiin perehtymään muutamiin järjestelmiin tarkemmin ja luotiin niistä yleiskuvaa antavia malleja. Tosibox -palvelinongelma poistettiin virtualisoimalla VPN palvelin konesaliin, josta päästään L2L VPN tunnelin kautta hallinnoimaan koululla sijaitsevia järjestelmiä sekä konesaliin virtualisoituja palvelimia. Langattomien lukkojen kaistapäällekkäisyys ongelmat ratkaistiin jättämällä 2.4 Ghz:n Opetusverkosta kanava 11 käyttämättä, jolloin taajuudet jäivät vapaiksi lukkojen Zigbee taajuuksille. Ratkaisu saattaa vaikuttaa negatiivisesti langattoman opetusverkon toimintaan, mutta ohjeessa sivuutettiin tätä painottamalla 5 Ghz:n taajuuksien käyttöä enemmän.

Tietoverkon jakamiseen tilaajan ja järjestelmien ylläpitäjän välillä pyrittiin tuomaan ratkaisu jakamalla tietoverkko virtuaalisiin segmentteihin, joista oikeudet toisiin ovat rajoitetut. Toteutuksessa tilaajan ja järjestelmien ylläpitäjän yhdistää konesalissa sijaitseva VPN -palvelin, johon molemmat osapuolet tarvitsevat yhteydet. Kuitenkaan

VPN:n kautta ei päästä näkemään koulun opetusverkon sisältöä, vain pelkästään ylläpidossa olevia teknisiä järjestelmiä. Tällöin ei tarvitse rakentaa kahta tai useaa fyysisesti erillään olevaa verkkoa, vaan voidaan rakentaa yksi tietoturvallinen ja toimiva tietoverkko. Virtualisoimalla palvelimia konesaliin voidaan myös eliminoida suurin osa paikallisista palvelimista.

Audiovisuaalisiin ratkaisuihin liittyviin ongelmiin myös pyrittiin löytämään ratkaisut. Tärkeänä osana tässä oli NVX järjestelmässä testatun ja suositellun kytkinmallin käyttäminen. Crestron järjestelmä pyrittiin saamaan toimivaksi molemmista verkoista, langattomasta sekä kiinteästä verkosta, käyttämällä laitteita ”Infrastructure” tilassa, jolloin ne yhdistettiin molempiin verkkoihin. Näin laitteet pitäisi olla käytettävissä molemmista verkoista. Tämän toiminnallisuutta ei kuitenkaan myöskään testattu.

7.3 Rajallisuus ja vaikeudet

Erilaisia järjestelmiä sekä järjestelmävalmistajia on todella suuri määrä, eikä läheskään kaikkea voitu avata tutkimuksessa sen laajuuden puitteissa. Valittiin siis muutamia järjestelmiä useiden joukosta, joita avattiin tarkemmin. Kuitenkin lähes minkä tahansa järjestelmän pystyy avaamaan tietoverkon näkökulmasta samalla tavalla, mikäli sitä pääsee itse testaamaan, tai jos siihen löytyy hyvät dokumentaatiot. Vaikeaa oli erityisesti kaikkiin järjestelmiin tarkasti perehtyminen ja toiminnan ymmärtäminen ilman järjestelmän testaamista. Toinen vaikeaksi koettu asia oli rajan vetäminen järjestelmien, sekä perinteisen tietoverkkosuunnittelun välille, joten huomioon otettiin vähän molempia.

7.4 Jatkokehitys

Tutkimus luotiin pohjaksi tietoverkkosuunnittelulle etenkin järjestelmien näkökulmasta, ja sen tarkoituksena on erityisesti se, että sitä voi kehittää eteenpäin. Esimerkiksi rakennusautomaatiojärjestelmiä ei käsitelty tutkimuksessa sen laajuuden vuoksi. Kuitenkin ohje on pyritty luomaan siten että sen avulla voi kartoittaa myös muita järjestelmiä, ja esimerkiksi rakennusautomaatiojärjestelmät voisi olla jatkossa kehitettävä kohde. Ohjeessa esiteltiin muutama järjestelmä esimerkkinä, ja samoilla

tekniikoilla voisi kartoittaa minkä tahansa muun järjestelmän. Järjestelmiä tulee kokoajan lisää sekä testauksessa ja käytännössä opitut asiat ovat todella arvokas lisä.

Lähteet

3-Series® Control Systems. 2019. PDF -dokumentti crestron.com verkkosivustolla. Viitattu 19.11.2019. https://www.crestron.com/getmedia/3672b6aa-80c6-49fd-959d-3a2e1ae22d8a/mg_rg_3-series_control_systems.

10 Gbps Cabling. N.d. PDF -dokumentti cisco.com verkkosivustolla. Viitattu 27.9.2019. https://www.cisco.com/c/dam/global/da_dk/assets/docs/presentations/10_Gbps_Cabling_0109.pdf.

910 Router. 2019. Datalehti -PDF helvar.com verkkosivustolla 24.4.2019. Viitattu 23.10.2019. https://www.helvar.com/media/pd/2019/20190703/910_DATASHEET_EN.pdf.

920 Router. 2019. Datalehti -PDF helvar.com verkkosivustolla 29.4.2019. Viitattu 23.10.2019. https://www.helvar.com/media/pd/2019/20190703/920_DATASHEET_EN.pdf.

Access. 2015. PDF -dokumentti lenel.com verkkosivustolla. Viitattu 8.10.2019. https://www.lenel.com/assets/library/onguard/OG_SS_AC_new%20format.pdf.

Ann Earon, S. N.d. Understanding & Evaluating AV-over-IP. PDF -dokumentti crestron.com verkkosivustolla. Viitattu 19.11.2019. https://www.crestron.com/getmedia/b6a586ce-9c00-4e50-ac64-9d844881ef6d/wm_av-over-ip_whitepaper.

Aperio™ AH30 -keskitin jopa 8 langattomalle ovelle. N.d. PDF -dokumentti abloy.fi sivustolla. Viitattu 8.10.2019. https://www.abloy.fi/Abloy/Abloy.fi%20(OW2)/Tuotteet/Tuotekatalogi/Elektroniset%20lukitusj%c3%a4rjestelm%c3%a4t/APERIO/Esitteet/WEB_Aperio_keskitin.pdf.

Appendix A: Allowed Wi-Fi Channels. N.d. Dokumentti arubanetworks.com verkkosivustolla. Viitattu 14.10.2019. https://www.arubanetworks.com/vrd/OutdoorMIMOVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=OutdoorMIMOVRD&file=AppA.html.

Assa Abloy Aperio Locks. 2014. Ohjedokumentti kb.lenel.com verkkosivustolla 2014. Viitattu 8.10.2019. http://kb.lenel.com/display/2/index.aspx?tab=opt1.

Bridging Traffic. N.d. PDF -dokumentti cisco.com verkkosivustolla. Viitattu 23.10.2019. https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA2_3_0/configuration/rtg_brdg/guide/rtbrgdgd/bridge.pdf.

Caverion lyhyesti. 2019. Artikkeli caverion.fi verkkosivustolla. Viitattu 12.12.2019. https://www.caverion.fi/tietoa-caverionista/caverion-lyhyesti.

Channel Planning Best Practises. N.d. Dokumentti documentation.meraki.com verkkosivustolla. Viitattu 11.10.2019. https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Channel_Planning_Best_Practices.

Channels, Zigbee. 2018. Dokumentti digi.com verkkosivustolla. Viitattu 18.11.2019. https://www.digi.com/resources/documentation/digidocs/90001537/references/r_channels_zigbee.htm.

Chapter: Configuring Bridged Mode. 2018. Artikkeli cisco.com verkkosivustolla 17.2.2018. Viitattu 23.10.2019. https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/getting/started/guide/ace_module_gsg/bridge.html.

Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. 2014. Artikkeli ciscopress verkkosivustolla 9.5.2014. Viitattu 17.9.2019. https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4.

Crestron® DigitalMedia™ System. 2019. PDF -dokumentti crestron.com verkkosivustolla. Viitattu 19.11.2019. https://www.crestron.com/getmedia/f32a4b5f-aaf2-421b-bf5a-7c8d715db041/mg_dg_crestron_digitalmedia.

DALI - Digital Addressable Lighting Interface. 2019. Tuotesivu helvar.com verkkosivustolla. Viitattu 23.10.2019. https://www.helvar.com/en/dali-products/.

Difference Between OS1 and OS2 Single Mode Fiber Cable. 2015. Artikkeli cable-solutions.com -verkkosivustolla 11.8.2015. Viitattu 9.10.2019. http://www.cables-solutions.com/difference-between-os1-and-os2-single-mode-fiber-cable.html.

DM-MD8X8-CPU3. 2019. Tuotesivu crestron.com verkkosivustolla. Viitattu 19.11.2019. https://www.crestron.com/en-US/Products/Video/DigitalMedia-Modular-Matrix/Switcher-Chassis/DM-MD8X8-CPU3.

DM NVX Application Design Guide. 2018. PDF -dokumentti crestron.com verkkosivustolla. Viitattu 19.11.2019. https://www.crestron.com/getmedia/154731bd-b79d-45b1-8b58-33feda6fa802/mg_design_guide_dm_nvx.

DM NVX™ AV-over-IP System. 2019. PDF -dokumentti crestron.com verkkosivustolla. Viitattu 19.11.2019. https://www.crestron.com/getmedia/fe0cf130-9884-42c7-bb62-7900148e619b/mg_dg_dm_nvx_system.

Education Solutions. 2019. Artikkeli crestron.com verkkosivustolla. Viitattu 4.11.2019. https://www.crestron.com/en-US/solutions/market/classroom-campus-room-building-automation-management-k-12-university.

Flatman, A. 2013. ISO/IEC TR 11801 ISO/IEC TR 11801-99-1 Guidance on 40GBASE Guidance on 40GBASE-T Cabling. Ohjedokumentti ieee802.org -sivustolla. Viitattu 27.9.2019. http://www.ieee802.org/3/bq/public/may13/flatman_01_0513_40GBT.pdf.

Fox, C. Jones, R. 2016. The Broadband Imperative II: Equitable Access for Learning. PDF-Dokumentti setda.org -sivustolla. Viitattu 30.10.2019. https://www.setda.org/wp-content/uploads/2016/09/SETDA-Broadband-ImperativeII-Full-Document-Sept-8-2016.pdf.

HD-RX-4K-410-C-E. 2019. Tuotesivu crestron.com verkkosivustolla. Viitattu 19.11.2019. https://crestron.com/en-US/Products/Video/HDMI-Solutions/HDMI-Extenders/HD-RX-4K-410-C-E.

HD-TX-101-C-1G-E-B-T. 2019. Tuotesivu crestron.com verkkosivustolla. Viitattu 19.11.2019. https://crestron.com/en-US/Products/Video/HDMI-Solutions/HDMI-Extenders/HD-TX-101-C-1G-E-B-T.

High Performance Collaboration. 2019. Artikkeli wolfvision.com verkkosivustolla. Viitattu 31.10.2019. https://wolfvision.com/vsolution/index.php/en/presentation-systems/cynap/cynap.

How Cisco IT Uses NetFlow to Improve Network Capacity Planning. N.d. Artikkeli cisco.com verkkosivustolla. Viitattu 30.10.2019. https://www.cisco.com/c/en/us/about/cisco-on-cisco/enterprise-networks/network-capacity-planning-web.html.

IEEE Std 802.3an:2006. Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. Aihealueet: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T. New York: IEEE Computer Society. Vahvistettu 1.9.2006. Viitattu 26.9.2019. https://ja-net.finna.fi, IEEE Xplore Digital Library.

Imagine. 2019. Tuotesivu helvar.com verkkosivustolla. Viitattu 23.10.2019. https://www.helvar.com/fi/ratkaisut/imagine/.

JHS 179 Kokonaisarkkitehtuurin suunnittelu ja kehittäminen. 2017. PDF -Dokumentti jhs-suositukset verkkosivulla 7.2.2017. Viitattu 18.9.2019. http://docs.jhs-suositukset.fi/jhs-suositukset/JHS179/JHS179.pdf.

Koulun historia. 2017. Artikkeli kokkola.fi verkkosivustolla 27.2.2017. Viitattu 15.10.2019. https://www.kokkola.fi/palvelut/opetus_ja_kasvatus/perusopetus/luokat_1_9_fi/torkinmaen_koulu/fi_FI/koulun_historia/.

Kupari, V. 2018. DALI-valaistusohjausjärjestelmän ohjelmointi oppilaitoskiinteistössä. Opinnäytetyö, AMK. Kaakkois-Suomen ammattikorkeakoulu, Sähkö- ja automaatiotekniikka. Viitattu 23.10.2019. http://urn.fi/URN:NBN:fi:amk-201802082155.

LNL-X4420. 2018. PDF -dokumentti lenel.com verkkosivustolla 11.2018. Viitattu 8.10.2019. https://www.lenel.com/assets/library/access-hardware/GSP-2716_LNL-X4420_ds%20web.pdf.

LNL-3300. 2017. PDF -dokumentti lenel.com verkkosivustolla 12.2017. Viitattu 8.10.2019. https://www.lenel.com/assets/library/access-hardware/GSP-2463%20LNL-3300%20DS%20web.pdf.

LNL-1300 Series 2. 2014. PDF -dokumentti lenel.com verkkosivustolla 2014. Viitattu 8.10.2019. https://www.lenel.com/assets/library/access-hardware/LNL_TS_1300s2.pdf.

McGrath, A. Bhaumik, S. 2013. Differences between OM1, OM2, OM3, OM4, OS1, OS2 fiber optic cable nomenclatures. PDF -Dokumentti stl.tech -sivustolla. Viitattu 9.10.2019. https://www.stl.tech/connectivity-solution/optical-fibre/pdf/Differences_between_OM1__OM2__OM3__OM4_.pdf.

Multi-SSID Deployment Considerations. N.d. Dokumentti documentation.meraki.com -verkkosivustolla. Viitattu 14.10.2019. https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Multi-SSID_Deployment_Considerations.

Murtoniemi, S. 2018. DALI-reititinjärjestelmän suunnittelu ja käyttöönotto. Opinnäytetyö, AMK. Kaakkois-Suomen ammattikorkeakoulu, Sähkö- ja automaatiotekniikka. Viitattu 23.10.2019. http://urn.fi/URN:NBN:fi:amk-201803263802.

Network Management System. 2018. Artikkeli cisco.com verkkosivustolla. Viitattu 10.12.2019. https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice.html.

News & Events. 2018. Artikkeli lenel.com verkkosivustolla 27.9.2018. Viitattu 8.10.2019. https://www.lenel.com/news-events/lenels-onguard-version-75-delivers.

OnGuard Version 7.5. 2018. PDF -dokumentti lenel.com verkkosivustolla 11.2018. Viitattu 8.10.2019. https://www.lenel.com/assets/library/onguard/OnGuard%207.5%20Data%20Sheet.pdf.

Planning for network availability. N.d. Artikkeli IBM verkkosivustolla. Viitattu 20.9.2019. https://www.ibm.com/support/knowledgecenter/en/POWER5/iphae_p5/highavailability.html.

Theiner, R. 2018. vSolution Cynap Network Integration. PDF-Dokumentti wolfvision.com -sivustolla. Viitattu 31.10.2019. https://www.wolfvision.com/wolf/Cynap_Network_Integration_en.pdf.

Tuotteet. 2019. Tuotesivu helvar.com verkkosivustolla. Viitattu 23.10.2019. https://www.helvar.com/fi/tuotteet/.

vSolution MATRIX. 2019. Artikkeli wolfvision.com verkkosivustolla. Viitattu 11.11.2019. https://wolfvision.com/vsolution/index.php/en/presentation-systems/cynap/vsolution-matrix.

What Is Network Security?. N.d. Artikkeli cisco.com verkkosivustolla. Viitattu 10.12.2019. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

Liitteet

Liite 1. Lenel -kulunvalvontajärjestelmän vaatimukset

LENEL -kulunvalvonta	Palvelin	Kontrolleri	Hubit - lukot	Hall. PC
Määrä	1	2	10 - 20	1
Tehtävä	järjestelmän aivot	lukee oi- keudet pal-	kommunikoi langattomasti	Moni- torointi
Internet, Kyllä/Ei	Ei	Ei	Ei	Ei
DHCP/Staattinen osoite	staattinen	staattinen	RS485	Staattinen
DNS record	ei	ei	ei	Kyllä
NAT	ei	ei	ei	ei
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)	ei	ei	ei	vain VPN kautta
Viive kriittisyys	alle 100ms	alle 100ms	alle 100ms	Ei
Kuorma verkolle (Per laite, arvio)	hyvin pieni	hyvin pieni	hyvin pieni	hyvin pieni
Liityntätekniikka, RJ45/WLAN	Ethernet	Ethernet + Rs485	RS485 - Zigbee	Ethernet
Tuetut kanavat (Jos WLAN)	-	-	11-26	

Liite 2. Kameravalvontajärjestelmän vaatimukset

Kameravalvonta	NVR tallennin	Kamera	Monitorointi pc
Määrä	1	15	1
Tehtävä	Tallentaa videot	lähettää kuva -> NVR	katsella NVR:ltä kameroita
Internet, Kyllä/Ei	Ei	Ei	Kyllä
DHCP/Staattinen osoite	staattinen	staattinen	staattinen
DNS record	kyllä	ei	ei
NAT	ei	ei	kyllä
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)	ei	ei	ei
Viive kriittisyys	ei	ei	ei
Kuorma verkolle (Per laite, arvio)	sisään n * 7mbit/s	7Mbit/s	normaali käyttökuorma
Liityntätekniikka, RJ45/WLAN	Ethernet	Ethernet	Ethernet
Tuetut kanavat (Jos WLAN)	-	-	-

Liite 3. Valaistusjärjestelmän vaatimukset

Valastusjärjestelmä	Dali reititin	Hallinta PC
Määrä	30	1
Tehtävä	Ohjailla valaisimia, jutella hallinta PC:lle	Ohjata reitittimiä
Internet, Kyllä/Ei	Ei	Ei
DHCP/Staattinen osoite	staattinen	staattinen
DNS record	ei	kyllä
NAT	ei	ei
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)	ei	vain VPN kautta sisäverkkoon, josta RDC hallinta PC:lle
Viive kriittisyys	ei	ei
Kuorma verkolle (Per laite, arvio)	hyvin pientä	hyvin pientä
Liityntätekniikka, RJ45/WLAN	Ethernet	Ethernet
Tuetut kanavat (Jos WLAN)	-	-

Liite 4. Cynap AV -järjestelmän vaatimukset

Cynap AV	Cynap	Keskuslaite	Käyttäjän laite
Määrä	34	1	n
Tehtävä	Toistaa kuva näytöltä	hallita cy-nappeja	lähettää kuva - cynap
Internet, Kyllä/Ei	Kyllä	Kyllä	Kyllä
DHCP/Staattinen osoite	DHCP	DHCP	DHCP
DNS record	ei	ei	ei
NAT	kyllä	kyllä	kyllä
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW pal-velin)	ei	ei	ei
Viive kriittisyys	mahd. pieni	mahd. pieni	mahd. pieni
Kuorma verkolle (Per laite, arvio)	sisään/ulos n. 14Mbit/s(video)	n. 15Mbit/s	normaali käyttö-kuorma
Liityntätekniikka, RJ45/WLAN	Ethernet + WLAN	Ethernet + WLAN	Ethernet + WLAN
Tuetut kanavat (Jos WLAN)	2.4 / 5 Ghz	2.4 / 5 Ghz	2.4 / 5 Ghz

Liite 5. Crestron NVX AV -järjestelmän vaatimukset

NVX AV	NVX	Hallintalaite	Käyttäjän laite
Määrä	8	1	n
Tehtävä	Toistaa kuva näytölle	viedä kuvaa nvx:ille	lähettää kuva tai sisältö – cp3n
Internet, Kyllä/Ei	ei	ei	Kyllä
DHCP/Staattinen osoite	DHCP	staattinen	DHCP
DNS record	ei	kyllä	ei
NAT	ei	ei	kyllä
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)	ei	Vain VPN kautta	ei
Viive kriittisyys	kriittinen	mahd. pieni	mahd. pieni
Kuorma verkolle (Per laite, arvio)	kuorma < 1Gbit/s	kuorma < 1Gbit/s	normaali käyttökuorma
Liityntätekniikka, RJ45/WLAN	Ethernet	Ethernet	Ethernet + WLAN
Tuetut kanavat (Jos WLAN)	-	-	2.4 / 5 Ghz

Liite 6. Kiinteän opetusverkon vaatimukset

Kiinteä opetusverkko	Työasema
Määrä	100
Tehtävä	Tarjota kiinteä yhteys opetus-verkkoon ja Internettiin.
Internet, Kyllä/Ei	Kyllä
DHCP/Staattinen osoite	DHCP
DNS record	ei
NAT	Kyllä
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)	ei
Viive kriittisyys	ei
Kuorma verkolle (Per laite, arvio)	1.5 – 4.3 Mbit/s
Liityntätekniikka, RJ45/WLAN	Ethernet
Tuetut kanavat (Jos WLAN)	-

Liite 7. Langattoman verkon vaatimukset

Langaton verkko	Tukiasema	Päätelaite
Määrä	22	n. 300-400
Tehtävä	Jakaa langaton verkko laitteille	päästä Internettiin ja resursseihin
Internet, Kyllä/Ei		Kyllä
DHCP/Staattinen osoite	Siltaava	DHCP
DNS record	ei	ei
NAT		kyllä
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)	ei	ei
Viive kriittisyys	ei	ei
Kuorma verkolle (Per laite, arvio)		1.5 – 4.3 Mbit/s
Liityntätekniikka, RJ45/WLAN	Ethernet	WLAN
Tuetut kanavat (Jos WLAN)	Jakaa	2.4 / 5.0 Ghz

Liite 8. Projektorijärjestelmän vaatimukset

Projektorijärjestelmä	Projektori	Hallinta-asema
Määrä	14	n
Tehtävä	Näyttää sisältöä kalvolta	hallita kaikkia projektoreita ohjelmalla
Internet, Kyllä/Ei	ei	Kyllä
DHCP/Staattinen osoite	staattinen	DHCP
DNS record	ei	ei
NAT	ei	kyllä
Pääsy ulkoverkosta, Kyllä/Ei (Esim. WWW palvelin)	ei	ei
Viive kriittisyys	ei	ei
Kuorma verkolle (Per laite, arvio)	?	1.5 – 4.3 Mbit/s
Liityntätekniikka, RJ45/WLAN	Ethernet	WLAN, Ethernet
Tuetut kanavat (Jos WLAN)		2.4 / 5.0 Ghz